University of Huddersfield

Factors that shape cybercrime victimisation and use of prevention measures in England and Wales

A thesis submitted in accordance with the requirements of The University of Huddersfield for the degree of Master of Science in Criminal Justice

Arturs Habirovs

Submitted in September 2018

Contents

List of Figures

Descriptive analyses:

Cross-variable analyses:

Regression analyses:

ABSTRACT

Cyberspace in general, and cybercrime in particular, are relatively new phenomena. As technological progress continues, the internet develops with it. In today's society, the majority of people are exposed to the cyberspace in the form of the internet and, subsequently, are potential victims of cybercrime. With this prevalence of the internet in people's everyday life, the issue of cybercrime should be acknowledged, addressed and explored more than ever.

The aim of this study is to explore current trends of cyberspace and crime committed within the internet environment. In particular, this research project aims to explore factors that shape victimisation and the use of prevention measures in cyberspace, with specific reference to extent to which people become victims of cybercrime and, moreover, use prevention measures to prevent such crimes in a cyber environment.

The issue described above is explored by conducting quantitative research analysing the general crime survey 'Crime Survey for England and Wales' (CSEW) on the matter of the internet and cybercrime. Exploratory analyses begin with descriptive statistics in order to review the current situation in cyberspace, followed by t-tests and regression analyses with the purpose to explore factors that might have an effect on cybercrime victimisation and the use of prevention measures in cyberspace. The results show that age is a relevant and significant factor when exploring both victimisation and the use of prevention measures in cyberspace.

On these grounds, it is recommended to consider age groups when developing cybercrime prevention strategies as well as for a further research project studying cybercrime victimisation rates. Additionally, it would be beneficial to explore how factors such as: the level of cybercrime 'worry'; cybercrime awareness and its relation to a number of prevention measures used; how often the internet is used; and income level; relate to victimisation and the use of prevention measures in cyberspace.

INTRODUCTION

The Information Age is a contemporary era in human history identified by the access and control of information and the subsequent transition from industrial production to computerised production (Rouse, 2014). This 'age of information' is associated with the invention of personal computers and, consequently, more advanced developments, such as microprocessors that can process enormous loads of information in very short periods of time and fibre optic internet cables that make it possible to transfer data at a speed of hundreds of megabytes per second. Such technological advancements allowed the general population to have access to the most modern pieces of technologies, such as smartphones which are now commonly used. In the 1950s, the world's first computer used to take up 160 square meters of space and was comparably limited in its processing potential. Just 60 years later, a smartphone that fits in a pocket has thousands of times more computing power than this first computer (Halfacree, 2014).

The first noteworthy cyber-attack or 'hack' that had a great impact on the world happened during Second World War in 1939 when Alan Turing and his team built the 'Bombe' device to decipher Germany's communications encryption code called 'Enigma' (Copeland, 2004). Later, in 1949, John von Neumann published a paper where he presented the 'computer virus' theory, where he speculated about computer programs' ability to reproduce themselves (Neumann, 1949); however, the theory did not come to practice until 1988 when Robert Tapan Morris programmed a 'worm' to exploit the first internet's UNIX system for scientific purposes. Nonetheless, in the 1990s, when the internet started to spread around developed countries, people found a way to abuse such 'worms' by programming them into harmful malwares. This is when hacking and cyber-attacks were born in a form that can be seen today.

The use of modern technology around the world has rapidly expanded in the last decade. In 2011, only 10% of people worldwide could state that they have personally used smartphones, while in 2018 that number has increased to 36%, equivalent to 2.53 billion people around the world (Statista, 2018a). It should be noted that most of the use of new technology takes place in the developed world. For example, in the United Kingdom (UK) smartphone ownership in 2017 has reached over 96% of the general population aged between 16 and 24 (Statista, 2018b). It can therefore be stated that the majority of UK residents are exposed to advanced technology, though it should not be assumed that everyone who owns a smartphone is exposed to the internet. Subsequently, they are exposed not only to the advantages of connectivity that these technologies offer but also to the issues that they can bring, many of which fall under the umbrella of computer and network-oriented crimes.

The phenomenon of cybercrime spread and escalated at a fast rate, alongside the expansion of cyberspace itself (Evans & Scott, 2017). Evans states that online fraud is the most prevalent offence in the UK, accounting for almost 50% of all crime. Unsurprisingly, fear of cybercrime is also becoming proportionately more common. Abel (2017) reports that, among US citizens, fear of identity theft through the internet exceeds the fear of a personal vehicle being stolen. His study finds that only 38% of Americans report a fear of their vehicle being stolen, while 66% worry about identity theft. Hence, it can be argued that the threat of cybercrime is real and that people appear to be concerned about cybervictimisation.

As such, the mechanisms behind fear of crime, specifically cybercrime, will be discussed. Virtanen (2017) argues that the impact of previous victimisation, as well as social and physical vulnerabilities, both play a role in shaping fear of cybercrime, similarly to other traditional crimes. According to Vanderveen (2006), fear of crime can be explained as an emotional response to a potential crime or the threat of physical harm, as well as a feeling of anxiety towards the phenomenon of crime or a symbol that an individual associates with a crime. Applying these definitions to the cybercrime issue, it can be argued that fear of cybercrime is constructed either by previous experience of cybercrime (emotional response to the possibility of cybercrime as a result of past harm caused by cybercrime) or by symbols that are associated with cybercrime (for example, media representation of cyber criminals and the current state of cybercrime, which might differ from reality). Earlier in the discussion, it was argued by Virtanen (2017) that previous victimisation affects fear of cybercrime in the same manner it affects fear of traditional crimes. The question of why people worry about cybercrime more than other crimes can be answered either by proving that people actually experience cybercrime much more than any other crimes, or by disproving it and leaving space for the effect of misrepresentation in media.

The purpose of this particular study is to shed light on a current situation in cyberspace in relation to use of the internet, actual victimisation rates online, and the effectiveness of prevention measures for individuals with different demographic factors in the UK. Current trends in cyberspace can be established by peoples' behaviour online. First of all, and most important, is to conclude whether the issue is relevant by exploring if people actually use the internet more and more over the years, whether people are getting more worried about cybercrime and whether this fear is justified by the actual cybercrime rates. Once descriptive data on internet use and fear of crime is obtained, it will become possible to track changes over the years amongst these variables and to conduct cross variable analyses in order to establish relationships between different factors and the effects those have had on internet users' behaviour online, fear of cybercrime and internet use. Furthermore, the regression analyses section will provide an insight into which variables are the most significant when exploring the shift in cyberspace trends.

The key aim of the study is to provide an insight into the current state of cyberspace in England and Wales and show how the internet impacts the lives of England and Wales residents. Moreover, the aim is to explore whether factors such as age, income or level of worry affect the total number of the respondents' victimisations. It would also be beneficial to explore relationship between use of the internet and concerns about safety in cyberspace assuming that people who are more worried use internet less. However, people might consider other factors more important than 'safety in cyberspace' and keep using the internet disregarding their concerns, because internet has become integral part of our lives and we use it for our most basic needs such as communication, shopping, banking etc. (SyndiGate Media Inc, 2018). Studying issues mentioned above will allow an opportunity to make practical recommendations on how to reduce victimisation in cyberspace. To help achieve the key aims of the study, in the 'Literature Review' chapter existing literature on the topic of cybercrime is reviewed and gaps in the existing knowledge on the matter are identified. Cybercrime extent is reviewed in the form of financial damage, percentage of internet users across the

general population, use of prevention measures and victimisation online, and criminological theories as well as theories built around cybercrime are discussed. The literature review section is followed by the 'Justification and Aims' section where the above-mentioned final aims of the study are identified. The 'Analyses' chapter will begin with the 'Methodology' section where the methods of producing the analyses are discussed and the decision-making process in relation to the data set is explained. The 'Methodology' section is followed by the main 'Data Analyses' section where all data manipulations are split into descriptive statistics, cross-variable analyses and regression analyses sections. Finally, analyses findings are discussed and explained relating to a previously reviewed literature in the 'Analyses Discussion' section, followed by the 'Conclusion' where the study is summarised and concluded.

LITERATURE REVIEW

Cybercrime – emergence and structure:

Technologies and communications are rapidly changing in modern times causing ever changing concepts of crime and criminality to adapt to an online world. The prevalence of technologies and the internet has radically changed the way we live, communicate, travel, share information, transfer funds, work and do business (Viano, 2017). To begin discussing cybercrime, victimisation online and use of cybercrime prevention methods it is crucial to understand how cyberspace emerged, extent of cyberspace and how it is regulated.

According to the United Nations Office on Drugs and Crime (2013), one third of the world population (2.3 billion people) have access to the Internet. Approximately 45% of all internet users are below the age of 25. As such, particularly for the younger cohort, it becomes more uncommon to encounter a crime that does not involve some elements of internet connectivity. The evolving environment of the internet and technologies makes planning and predictions around cybercrime uncertain, especially for law enforcements. As a result, the cybercrime field is often unregulated or regulated by outdated statutes that do not encompass the newer developments.

Cybercrimes with major impact have been occurring since the early years of the Internet; in May 2000, a computer virus called 'Love Bug' infected computers world-wide, including government agencies in the UK and US, resulting in estimated damage of between $7-10 billion. The prime suspect was a college dropout from the Philippines, however all charges were dropped and Onel de Guzman, suspected at the time, was not prosecuted, as the Philippines did not have any laws that covered computer hacking under which he could be prosecuted (Philippsohn, 2001).

Deloitte's report (2015) on cybersecurity trends states that cybercrime evolves alongside technologies and becomes increasingly more sophisticated. Hackers are not exploiting targets of opportunity anymore, instead they have the freedom to select specific individuals, companies or services that become available as victims trust more and more information to be secure on the Internet, which opens new opportunities for criminals. Another side of the

cyber environment that may cause potential issues is artificial intelligence and drones, which may be used as surveillance, violating people's privacy, or even as a lethal weapon. Graham (2016) provides an example of the use of a robot with a lethal outcome; in July 2016, Dallas, Texas, the police used a robot to find and eliminate a sniper who killed five police officers. Using robots to kill suspects is truly uncommon, however many police forces do often use remotely-controlled drones to defuse or detonate bombs.

Yar (2006) argues that the issue of cybercrime should have been addressed much earlier within the framework of sociology, psychology and criminology. The author states that the major issue for studying cybercrime is the absence of any current and consistent definitions of cybercrime. Wall (2001) notes that the term 'cybercrime' has no specific definition in law, however the term is often used in politics, media and within the criminal justice system. Yar suggests that instead of trying to conceptualise the term 'cybercrime' as a single phenomenon, it should be seen as a range of activities where networks of information and communication technology (ICT) or the internet are key variables. On the other hand, Thomas and Loader (2000) defined cybercrime as a conceptualised term – "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (Thomas & Loader, 2000, p. 3). The definition provided by academics touches upon a crucial distinction between crime (act prohibited by law) and deviance (act that breaches informal societal norms), which is important for further reflection on the definition.

Despite the efforts of many academics to reach a conclusive definition of the phenomenon, Wall (2008a) believes that there is still a gap in understanding how the term 'cybercrime' is constructed. The author claims that the law is lacking a clear definition of cybercrime, which leads to the public creating its own perception of what cybercrime is, subsequently creating many myths around cybercrime. Wall believes that the origins of cybercrime concepts lie in science fiction novels and films, which were the first sources of cyberspace visualisation. Another important factor, according to Wall, is the public's desire for newsworthy information, both a consequence of and incentive for the continuous production of 'shocking' content by the mass media, which explains news outlets sensationalising cybercrime. As an outcome, many myths are constructed around cybercrime, which creates erroneous perceptions of it among the public (Wall, 2008b). As a source of this mythology, the author reviews the abstract of the House of Lords Science and Technology select committee report (House of Lords, 2007, p. 6). For example, the myth of an 'omnipotent super-hacker' who is aware of legal loopholes and is impossible to trace. Kevin Mitnick, who was the face of the 'omnipotent super-hacker' in the 1990s, deconstructed his own myth explaining that at the time security levels were much lower than today. Simple login details such as username 'Admin' and password 'Admin' were common, and basic social engineering moves such as persuading low-level employees and accessing their access codes were not difficult to achieve (Mitnick & Simon, 2002). These myths were constructed in the early ages of the internet and created some beliefs around cyberspace, which still affect the current public perceptions of cybercrime, as well as the recognition of cybercrime as a real threat. On the other hand, Singleton (2013) argues that the threat of cybercrime is quickly spreading and escalating. The author states that an increased usage of the internet over the course of history created

favourable circumstances for criminals to switch from street crimes to cybercrimes because it is safer, it does not depend on geographic location and the internet provides more opportunities – such as vulnerable internet users. As an example of organised crime against the government, Singleton discusses the 'false refund scheme' cybercrime where cybercriminals used to steal funds from the government by filing tax returns with false information. The cost of such cybercrime to the U.S. in 2012 was $5.2 billion. Likewise, most common cybercrime against individuals is ID theft. According to the Federal Trade Commission's (FTC) survey of fraud in the United States (Federal Trade Commission, 2013), during 2011 an estimated 25.6 million adults, which is almost 11% of the adult population in the U.S., were fraud victims.

Summing up the arguments discussed above, it can be concluded that cybercrime is a truly uncertain phenomenon that evolves at a very fast pace. The structure of this study's analyses is based on uncertainty, a fast-changing environment and the fact that the extent of cybercrime is often measured by financial impact on the country, which might not usually represent actual impact of cybercrime on the general population, which could be measured more accurately by analysing self-reported victimisation rates. It is crucial to establish actual use of the internet, levels of worry about cybercrime and actual victimisation rates across the general population.

Owen, Noble and Speed (2017), members of the UCLan Cybercrime Research Unit (UCRU) at the University of Central Lancashire, provided some of the most contemporary work addressing more current gaps in the criminological theory on cybercrime. The authors look at the issue of cybercrime from various angles, attempting to demonstrate that cybercrime must be seen as an interdisciplinary issue. Elements of cybercrime such as the laws governing it, the ways cyberspace is regulated, deviance, and identity in cyberspace are reviewed in the paper from the perspectives of criminology, sociology, philosophy, computer science and other fields of social and applied sciences. This work truly displays how complicated cybercrime can be and why it should be addressed from different points of view and different philosophical angles due to its ever-changing nature.

One way of looking at cybercrime within the field of criminology is through the application of traditional cybercrime theories, which many authors have subscribed to. Choi (2011) applied Cohen and Felson's (1979) Routine Activity Theory (RAT) to cybercrimes, trying to examine which factors are responsible for cybercrime victimisation. For RAT to work there are three main factors that need to be present at the same time for victimisation to occur: an interested offender, an opportune target and the absence of a capable guardian. Choi used these principles to conduct a study of victimisation in cyberspace and found that different lifestyle patterns are linked directly with being victimised in cyberspace. The author also states that McQuade (2006) suggested these findings earlier and criminal justice crime-prevention programs ignored them. Furthermore, Holt and Bossler (2009) applied RAT to one particular form of cybercrime – online harassment. As research outcomes, the academics made several conclusions. First, routine computer use and physical guardianship had little influence on online harassment victimisations. Second, engaging in deviant activities in cyberspace increases the risk of victimisation. Kigerl (2012) takes another perspective and applies RAT to

cybercrime on a national rather than an individual level. The aim of his research was to discover the most accurate predictors of high cybercrime activity in any particular country. Using a sample of 132 countries, the researcher was able to conclude that wealthier nations had higher cybercrime activity rates, largely as a consequence of more people having access to the internet. However, the author also argued that unemployment increased rates of cybercrime engagement (Kigerl, 2012).

Another way of understanding the cybercrime phenomenon is by examining the key regulations and laws around cybercrime and their changes over time. Griffin (2012) argues that cybercrime is a truly underexplored field, with many challenges and issues that need to be addressed. The author speaks about cyberspace aspects such as privacy, anonymity and rights and proposes ways in which laws may be structured around these principles to better apply to cybercrime cases and discusses the ways they are handled from a legal perspective. As an example, Gray, Citron and Rinehart (2013) reviewed the case of United States v. Jones from the perspective of privacy in cyberspace. The Fourth Amendment in the U.S. constitution implies that an individual has the right to privacy and therefore the offender could not be prosecuted because, in the course of the investigation, the government would be invading the offender's privacy in order to gather evidence against him. Academics discuss this issue and how privacy can be addressed in cyberspace from the perspective of law. Furthermore, Dobrinoiu (2014) discussed how laws are addressed with regards to ID thefts in Romania. ID theft crimes became more prevalent with cyberspace opening up new opportunities for criminals, alongside which laws were adapting, though not quickly enough. The author discusses the flaws in legislation with reference to different law articles and states that there is too much room for misunderstanding and misinterpreting laws related to ID theft crimes.

According to Wall (2015), people have started to acknowledge that cybercrime exists, and that it possesses a real threat, however, when cases of cybercrime are brought to court, they are still most likely to be reviewed as 'traditional' rather than 'cyber' crimes. The author claims that the state of things related to cybercrime is definitely improving, but there are still numerous challenges that need to be addressed. Baines (2013) provides an example of cybercrime becoming viewed as a real threat and has started to be properly addressed. In January 2013, the European Cybercrime Centre (EC3) was established as a part of Europol in The Hague to address the issue of cybercrime in European Union member states. In 2014, Interpol's new department, the Digital Crime Centre, became operational, with aims to target cybercrimes across different industries such as academia, civil society organisations and government authorities. Nonetheless, the issue of cybercrime still needs to be addressed from the perspective of the general population as not only organisations and authorities are affected by cyber-attacks. The focus of this study is going to be aimed on the general population because people still experience cyber-attacks, though this part of the cybercrime issue gets insufficient attention.

Personal Electronic Devices – use over time:

Over the last couple of decades, use of mobile computing technologies has been significantly increasing (Ladd, Datta, Sarker, & Yu, 2010). In this section, Personal Electronic Devices (PEDs) are going to be reviewed insofar as their connectivity to, and use of, the internet. For example, students who use PEDs for studies most likely use devices such as smartphones or laptops to access the internet for information. Medical personnel are likely to use PEDs in working conditions to communicate or access information about patients. Using PEDs in the modern world implies use of the internet in most cases.

Smartphones especially possess the unique combination of technologies such as digital cameras, online messengers, music and multimedia content, and it is known that their presence and use have shifted human interactions in the society (Koo, Chung, & Kim, 2015), subsequently allowing for more complex cybercrimes to take place. For example, in 2013 in the U.S., 70% of all mobile devices were smartphones (Hardawar, 2012). Even within the field of academia, Hossain and Ahmed (2016) studied the use of smartphones by university students in Bangladesh and found out that the vast majority of students were using smartphones for academic purposes. Moreover, scholars found that the use of academic smartphone applications by students to support their learning needs has also been increasing (Woodcock, Middletion, & Nortcliffe, 2012). Bomhold (2013) found that 76% of U.S. undergraduate students use smartphones to find academic information. A similar study on medical students in a Parisian university showed that only 3.3% of respondents did not use mobile devices in clinical workplaces to access medically-related or other information (Scott, Nerminathan, Alexander, Phelps, & Harrison, 2017). Another study also shows that nowadays over 95% of young adults in the U.S. have a smartphone and, furthermore, 30% of them state that they 'cannot live' without a smartphone (Gibson, 2014).

The above-mentioned studies have shown that use of personal electronic devices (PEDs) over time has been increasing. Nonetheless, it can be discussed how PEDs are being integrated in our everyday lives and whether smartphones are beneficial or not. Chen and Ji (2015) argued that many researches have been studying the widespread use of smartphones and personal electronic devices amongst students, however, the ways smartphones affect students' thinking styles have not yet been considered. The academics found out that the use of smartphones for academic purposes positively affected their performance, however, students who used smartphones for non-academic purposes performed worse. Wang, Xiang and Fesenmaier (2014) have discussed how smartphones have been changing aspects of our everyday life in an example of U.S. travellers. By virtue of smartphone applications, where travel options such as trains, planes and hotels are in one place, tourism becomes more accessible and decision-making processes become easier, changing the shape of consumerism. Similarly, Fuentes and Svingstedt (2017) explored how the introduction of smartphones had changed the shopping habits of the general population. Smartphones positively affect the shopping experience for consumers, providing them with new opportunities and more options, subsequently allowing consumers to compare prices, which opens up a new perspective on the economy (Kourouthanassis & Giaglis, 2012). As a disadvantage, Kourouthanassis and Giaglis (2012) state that the introduction of smartphones

to the shopping experience may cause consumers to experience stress and anxiety as a consequence of such a wide choice of products as well as opening new cybercrime opportunities.

Another important field where the internet and PEDs are being heavily relied on in the modern day is medicine. People have begun to trust their most private information such as healthcare records to the internet, which makes the issue of cybercrime even more delicate. Koivunen, Niemi and Hupli (2015) studied how electronic devices are being implemented into healthcare professionals' communication process. PEDs and the internet opened new opportunities for communication, which is particularly important for healthcare personnel. The researchers found that new online communication methods such as email and messenger applications on smartphones proved to be useful, improving personnel competences as well as the organisation of daily operations and administrative tasks. Nonetheless, it also raises questions relating to information security and provides new cybercrime opportunities. Going even deeper in the area of healthcare and use of PEDs, Mobasheri, Johnston, Syed, King and Darzi (2015) have explored how smartphones and tablet devices are being used during surgeries. Authors state that there are various ways of implementing PEDs in surgery, from operation planning and navigating to diagnostic and surgical training.

Smartphones and other PEDs have proved to be useful in improving quality of life for many people, however, the subject has also faced opposition. Škařupová, Ólafsson and Blinka (2015) studied the phenomenon of excessive internet use (EIU) in Europe. With the introduction of smartphones, internet activities such as online gaming and social networks have been brought into the lives of young people. Now, young people do not need to go somewhere for entertainment or to socialise because they have access to online entertainment in a form of online games and communication to other people in a form of social networks. With such activities brought to adolescents' lives they spend more and more time online rather than offline (Livingstone, Haddon, Gorzig, & Ólafsson, 2011). Spada (2014) states that problematic internet use (PIU) became a global and prevalent issue which can lead to negative consequences in daily life, such as neglecting real life social activities and relationships, negative impact on health and work duties and the alteration of sleep schedules and eating habits. The author also states that PIU might even be considered a psychiatric disorder, however further research is necessary. Spending more time online causes people to start becoming addicted to online activities, leading to serious issues such as, for instance, distraction-affected motor vehicle crashes. According to the National Highway Traffic Safety Administration (2016), distracted driving killed 3,179 people in the U.S. and injured an estimated 431,000 others in 2014. Additionally, text messaging while driving increases the likelihood of being involved in a safety-critical event 23.2 times (Olson, Hanowski, Hickman, & Bocanegra, 2009). Distraction amongst pedestrians is also a crucial safety risk, however it is difficult to estimate the number of accidents as a consequence of a distracted pedestrian. Another study related to the distraction-affected crashes was conducted in the Netherlands on a sample of bicyclists (Goldenbeld, Houtenbos, Ehlers, & De Waard, 2012). Academics studied different age groups of cyclists from 12 to 50+ years old and found that young adult cyclists (18-34 years) were more frequent PEDs users. Furthermore, the authors found that

teen cyclists and young adult cyclists who used electronic devices on every trip had a higher risk of being involved in a bicycle crash.

To summarise, the use of PEDs and the internet has increased over time, and these factors have positively affected human quality of life, but have also brought controversy and various possible health and safety issues. The takeaway point is that new cybercrime opportunities became accessible and people became more exposed to cybercrimes. However, the data mostly comes from the European countries or the U.S. and the topic is rarely explored within the UK.

Exposure to cybercrime:

The use of Internet and smartphones is becoming more prevalent and people unwillingly have to trust electronic devices with more and more personal information due to employment and social commitments, subsequently getting increasingly concerned about the safety of that information in cyberspace. According to a survey studying internet users within the European Union, 76% of respondents believed that their risk of cybercrime victimisation has increased (Baker, 2013). In spite of that fact, only 46% of respondents had changed any of their passwords during the past year and only 12% were victimised in a form of banking fraud online or had their email or social media accounts hacked. GFI Software Corporation (2015) conducted an independent study examining UK and U.S. citizens' concerns towards cybercrime. Results of the survey showed that 46% of respondents were victimised at least once in the past year. Another interesting finding is that 71.5% of the U.S. citizens believe that cybercriminals are a serious threat to the national security and half of the respondents stated that cybercrime makes their lives more difficult. Surveyors also state that findings in the U.S. can be projected to the UK demography, with a slight difference. Mesko and Bernik (2011) have also studied fear and awareness of cybercrime but in Slovenia. The authors state that the vast majority of 'fear of cybercrime' is caused by different myths that surround the topic, as well as inaccurate media representations (Wall D. S., 2008b). During a study in Slovenia, a correlation was established between fear of cybercrime and awareness of possible cybercrime consequences, and it was argued that fear of cybercrime is not dependent on the actual state of a crime (Mesko & Bernik, 2011). The authors also state that people in Slovenia are well informed about different types of cybercrime, however they are mostly aware of cybercrimes portrayed in the media rather than the ones they are more likely to be affected by.

Goucher (2010) analysed survey results where 65% out of approximately 77,000 respondents from different countries had been victims of cybercrime. The key result is that 26% of respondents felt 'helpless' as a consequence of cybercrime and furthermore, only 44% of them reported the crime to the police. This leads to the conclusion that either cybercrime is being addressed poorly, or people are simply not aware of the reality of cybercrime prevention, as 80% of respondents said that they did not expect perpetrators to get arrested. Hernandez-Castro and Boiten (2014) studied cybercrime prevalence in the UK, where approximately 80% of households had an internet connection in 2012 (UK: Office for National

Statistics, 2013). The researchers analysed the Crime Survey of England and Wales (CSEW) 2011/2012 sweep and found out that 37% of internet users reported being victimised in the form of a computer virus and unauthorized access of personal data, among others.

De Voe and Murphy (2011) provided an example of the scale cyber-bullying – a new type of crime emerging from widespread use of the internet and smartphones – can reach. Academics analysed statistical data collected by the National Crime Victimization Survey (NCVS) in the U.S. and figures showed that approximately 1,521,000 students were cyber-bullied on or off school property. Another piece of research, which explored cybercrime and the prevalence of internet and mobile devices, was conducted in Greece (Papanikolau, et al., 2013). Academics discussed statistics provided by the Ministry of Citizen Protection of the Greek Government and found that most cybercrime activities were committed through the Facebook social network. A majority (203 out of total 327) of cybercrimes committed through a use of Facebook are cases of potential suicide. Authors conclude the paper by stating that cybercrime will likely become one of the most dominant crimes as a result of the technological revolution.

Moving on, Leukfeldt (2014) provided a case study of a particular cybercrime called 'phishing' in Amsterdam. Phishing is defined as the act of stealing someone's digital credentials, for example credentials of online bank accounts. The researcher provided data on costs of phishing to banks in the Netherlands and the UK to display that the threat is real and phishing as a particular form of cybercrime is emerging. In the UK, banks lost an equivalent of 41.2 million euros in 2011, further reaching 46.2 million euros in 2012 (Financial Fraud Action UK, 2013). In the Netherlands in 2011 and 2012 the damage count had reached 35 million euros (Nederlandese Vereniging van Banken, 2012). Further in the paper, the author provides an in-depth case study on different forms and techniques of phishing and provides advice as to how the issue might be addressed. Dimc and Dobovsek (2013) studied the perceptions towards cybercrime of people in Slovenia and the U.S., focusing on the subject of cyber security awareness and actual behaviour in cyberspace. The authors concluded that there exists a difference between the level of awareness and level of actual implication of security methods. Another interesting finding by academics in the course of the research was that perceptions of safety in cyberspace depend on the physical location; respondents from a small country such as Slovenia felt safer than participants from the considerably larger U.S.

Another study of students' victimisation in the U.S. was conducted by Choi (2008) who was exploring how online behaviours affected the exposure to cybercrimes. He analysed self-report surveys, which included different questions related to subjects such as computer security measures, online lifestyle and cyberspace lifestyle. The author was able to provide empirical evidence that both behaviour in cyberspace and digital guardianship are important aspects when reviewing cybercrime victimisation, which consequently allowed for the application of RAT to cyberspace crimes. On the other hand, Jardine (2015) argues that the cybercrime is not as common as it is represented in different statistical reports and the author states that online victimization is relatively uncommon. He also states that the data on the occurrence of cybercrime is not accurately represented in the form of number of attacks per year and proposes that the extent of the data on cybercrime requires a shift in the focus

towards users, which should then be represented as occurrences per thousand people per year. Upon analysing IT firms' security reports from this perspective, he argued that the actual state of cyberspace is much safer than it is displayed in other sources and commonly thought.

Nasi, Oksanen, Keipi and Rasanen (2015) conducted a multi-national study (Finland, U.S., Germany and UK) using a sample size of 3506 people aged between 15 and 30 years old and based their statement of cybercrime being uncommon on that study; they also defined the most significant predictors of online victimisation as being: male, young age, immigrant, not active social life offline, urban residence and not living with parents. The authors further imply that RAT can be applied to cyberspace to explain victimisation. Another point of view on cybercrime rates being misrepresented and the actual state of cyberspace being better than generally perceived is provided by Bidgoli and Grossklags (2016), who believe that these statements are a consequence of cybercrime being underreported. Academics state that factors such as minor financial damage, psychological or emotional trauma as a consequence of committed crime being of highly sensitive nature, make certain types of cybercrime not being reported. Another important factor may be that victims are not aware of where and how to properly and effectively to report cybercrimes.

A different way of measuring cybercrime is the economic perspective on cybercrime damage. Figures and numbers of different governmental, international or bank sources can provide another perspective on cybercrime exposure. Armin *et al.* (2015) reviewed exposure to cybercrime from the economic perspective between 2010 and 2015 to predict the overall costs of cybercrime to the economy in 2020. The main aim of the study was to showcase the issues that cause damage to the economy and to provide advice on how to negate that damage in the next 5 years. Academics reviewed statistics on cybercrime from various sources and estimated that the damage to the global economy from cybercrime measures up to €300 billion per annum (McAfee & CSIS, 2014a). This may seem a sizable figure, but in proportion it only amounts to 0.4% of the EU's gross domestic product (GDP) value, equivalent to €13 billion (McAfee and CSIS, 2014b). Norton antivirus software company conducted its own research with a sample size of 24 different countries measuring the damage of cybercrime as a $110 billion a year. Researchers argue, however, that most cybercrimes remain unreported and, furthermore, many cybercrime victims are not even aware that they have been victimised (Norton Antivirus Software, 2012). A banking malware called 'Dridex botnet' is a practical example of the damage that can be caused to the economy. The National Crime Agency (NCA) in the UK stated that this type of botnet stole around £20 million from online bank accounts over the course of several months (National Crime Agency, 2015).

As it can be seen, 'botnets' is a costly and effective method of committing cybercrime defined as a network of infected computers controlled by a botnet commander to perform variety of cybercrimes (de Graaf, Shosha, & Gladyshev, 2012) such as distributed denial-of-service attacks (DDoS), bitcoin mining, spam, information stealing or click fraud (Wagenaar, 2012). Wagen (2015) also states that the botnet technique of cybercrime can be conceptualised from a criminological perspective by applying RAT and viewing cybercrime as a concurrence in space and time of a rational offender, suitable target and absence of guardian. Another way to appraise the issue is from the perspective of the Rational Choice Theory (RCT) which

emphasises the offender's decision-making process (Clarke & Cornish, 1986), where a rational offender creates the botnet tool for himself or others. On the other hand, Ngo and Paternoster (2011) also applied RAT to an issue of cybercrime victimisation by studying U.S. college students and concluded that neither individual nor situational factors consistently impacted on the likelihood of cybercrime victimisation. The authors state that a theoretical framework other than RAT should be applied in explaining victimisation in cyberspace. Moreover, Dupont (2017) focused on issues and limitations of enforcements in controlling and regulating major international cybercrimes, using the example of botnets. Dupont, however, only discusses three main approaches that were employed in fighting botnets: first, arresting hackers to cause a deterrent effect; second, developing software preventing attacks from happening; and third, governmental actions in the form of harm reduction and awareness raising. Analysing these approaches, scholars have concluded that there is not enough data available to evaluate the effectiveness of such approaches, as the vast majority of that data is within private organisations such as Internet Service Providers, software companies and search engine companies. Saying that, 'botnet' is only one of many issues that are considered when measuring financial cybercrime damage.

Despite the issue of a lack of data, the Ministry of Defense (MoD) in the UK believes that previous studies aimed at costs of cybercrime *overstated* the issue and did not differentiate between direct and indirect costs of the offence (Anderson, et al., 2013). As an example, the authors reviewed a large-scale botnet attack from 2010 where owners of the malware profited in just around $2.7 million while worldwide prevention expenditures were over a $1 billion. Therefore, while the impact of cybercrime can be measured in the perspective of economic damage to a country or the whole world, it should be done properly with a clear distinction between earnings of criminals and costs of prevention of these cybercrimes. In summary, people around the world are concerned about being victims of cybercrime and, upon exploring a wide variety of cybercrimes, it becomes apparent that the probability of being victimised in cyberspace is quite high. Discussing statistics on cybercrime exposure, it is important to keep in mind that exposure can be measured in different ways such as financial impact, police reported incidents, self-reported victimization incidents and unnoticed incidents. In a framework of this study cybercrime exposure is going to be measured in a form of self-reported victimization. To continue, the following section is going to cover the various ways this issue is being tackled.

Cybercrime prevention methods:

As previously established, people in contemporary society take advantage of technological progress and personal electronic devices, the internet specifically becoming an important feature of the everyday lives of a majority of people. Eddolls (2016) states that the cybercrime threat continually grows as a consequence of cybercriminals adapting to the contemporary security measures and users' online behaviour. The author argues that, regardless of the security measures implemented, criminals are always one step ahead; the reason behind this is that cybercrime is not being treated as it should be. Eddolls believes that cybercrime should be treated as an offence of the highest priority due to the damage it can cause. To get ahead

of cybercriminals, we must make cybercrime prevention the highest priority, judge the actual state of cybercrime realistically and employ proper cybercrime prevention methods. Akhgar and Brewster (2016) provided a collection of discussions on different topics surrounding cybercrime. The book is built as a roadmap to cybercrime prevention, starting with different trends and challenges of cybercrime and cyberterrorism, how it can be tackled from legal, ethical and privacy perspectives, how it can be tackled from a technological perspective, and finally a discussion of cybercrime research developments. Koops (2016) defines seven 'megatrends' of present-day society and technologies that can be summed up as the internet becoming the infrastructure of everything, the shifting paradigm of cybercrime, and the disintegration of privacy. On the background of these trends, the author proposes seven challenges to the security of society, such as underground marketplaces, preserving human rights, and the regulation and organization of cyberspace. Roosendaal, Kert, Lyle and Gasper (2016) discussed the application of laws and legal framework to data protection in cyberspace, considering how it would interact with other principles such as freedom of speech and academic freedom.

Before speaking of crime prevention techniques, it would be beneficial to address fear of crime (FOC) as a criminological concept. The emotion 'fear' can be seen as a mix of different feelings, risk-estimations and perceptions, meaning that fear is a very subjective emotion (Ditton, Bannister, Gilchrist, & Farrall, 1999). Furthermore, Wynne (2008) argues that fear is a natural response to crime. Gooch and Williams (2015) state that even though FOC might be genuine, it is often irrational because it is not based on a true analysis of a situation. For example, Gooch and Williams discussed situations with elderly people who were afraid to go outside because they feared being robbed. However, statistically, elderly people are less likely to be victimised in such a way. This kind of example could be applied theoretically in the cyber environment. The academics Roberts, Indermaur and Spiranovic (2013) analysed The Australian Survey of Social Attitudes of 2007 on the subject of how fear of cybercrime differs from fear of traditional crime and had concluded that worry of identity-related cybercrimes (such as stolen credit cards or other forms of identity theft) matches or exceeds worry of traditional place-based crimes.

Another important consideration in data protection laws discussion is the difference between countries. Choras, Kozik and Maciejewska (2016) discuss ways in which cyber security is emerging from technological perspectives and ways to push the progress of technological cybercrime prevention even further. The authors discuss examples of the most modern biological security measures, how these measures show positive impact on cybercrime exposure rates and how they can be implemented even further to be even more successful. And finally, Choras, Kozik, Churchill and Yautsiukhin (2016) presented a discussion of further possible developments in the vector of cybercrime prevention researches. The scholars review different projects that are aimed at cybercrime prevention, using different technological manipulations of modern electronic devices and online environment; through practical examples they provide arguments for further developments. Bernik (2014) has provided a book where he discussed methods of exploiting cyberspace. He has also argued that cybercrime could be prevented through intervention in technologies or by adjusting the laws regarding cybercrimes.

With regards to preventing cybercrime victimisation on a technological level, Reyns, Randa and Henson (2016) explored this topic and conducted research that was aimed at identifying factors that may affect preventative behaviour in cyberspace; they achieved this by examining relationships between exposure to cyberspace, cybercrime victimisation and online communication within an opportunity framework. The academics concluded that exposure to cyberspace and routine activities in online communication were predictors of cybercrime victimisation. Moreover, it was concluded that taking precautionary measures online negates the likelihood of cybercrime victimisation's underpinning thesis, which is that interaction in technologies might be effective in cybercrime prevention strategies. Mahoney (2016) provided practical tips on how to work with contemporary technologies to avoid victimisation. For instance, modern security measures such as two-factor authentication, which adds another layer of security on top of basic username and password in the form of a confirmation of login from mobile device, have proven effective. The author also states that another important behaviour to employ is to receive software updates only from trusted sources. Rughinis and Rughinis (2014) analysed results of a survey of internet users from different European Union countries on the subject of behaviour in cyberspace and cybercrime exposure within a framework of routine activities. The academics grouped respondents according to their online activities, cybercrime exposure and security measures employed and came up with five types: explorer, reactive, prudent, lucky and occasional. The authors concluded that separating online users into five groups can be useful for analysing which type of prevention techniques work and which type of strategies are designed wrong. They provide as an example: due to the fact that current cybercrime prevention campaigns are aimed at parents and young users who are 'explorer' and 'lucky' types, 'prudent' users, who make up the majority, do not usually have their concerns addressed within these prevention campaigns.

On the other hand, cybercrime could be addressed from a legislative point of view. It must be taken into consideration, however, that different countries adjust laws differently. In England and Wales, the main laws that cover cybercrime are the 'Computer Misuse Act' of 1990 and the 'Serious Crime Act' of 2015 that are being adjusted and developed in order to address the most contemporary cyber environment issues. However, in the Philippines for example, the Cybercrime Prevention Act was enacted only in 2012, when the State finally recognised the importance of the safety of information in cyberspace (Celine, 2013). First of all, the act addresses illegal access to a computer system, considering confidentiality and interceptions of any non-public transmissions. Secondly, it forbids categorised computer related frauds such as data forgery, alteration or deletion of data, identity theft and others. And finally, content related offences in a form of unsolicited commercials as well as defining all cybercrimes under existing laws are also addressed. Mayer (2016) argued against the current state of laws around cybercrime in the U.S., stating that federal statute and the Computer Fraud and Abuse Act could be adjusted. The author asserts that laws are too often aimed at low level crimes such as government employees mishandling data, which leaves serious gaps in law, allowing criminals to commit large scale cybercrimes that cause billions in damage yet are not being addressed. Mayer discusses different cybercrime laws and proposes adjustments that could be made to fill that gap.

Also regarding law adjustments, Fick (2009) states that to properly and effectively address cybercrime, legislative focus should fall on prevention rather than prosecution. Fick builds his thesis on the statement that prevention is much more effective than prosecution because of different factors discussed earlier such as the 'victimless' crime, victims not being aware of the crime, cybercrime being underreported, difficulties in tracing offenders, etc.

Even though some authors believe that technological interactions and law adjustments are the main approaches to preventing cybercrime, different countries and different organisations have experimented with other approaches. Buono (2014) discusses how cybercrime could be tackled through awareness raising. The article by Dimc and Dobosek (2013) that supports the thesis of awareness raising being an effective strategy was discussed earlier in the 'exposure' section. In summary, the main point of the article is to argue that cybercrime prevention through public campaigns on ways to protect yourself online and general cybercrime awareness raising strategies are effective. It is also brought up that the cybercrime legislation is still not sufficiently clear and comprehensive, and that cybercrime must be considered international. Kratchman, Smith and Smith (2008) have also discussed the perspective of prevention through awareness raising, but only at the level of companies and organizations. Considering the most prevalent cybercrimes (viruses and DDoS), it was proposed that the damage to different companies and organizations in the U.S. could be significantly minimised through awareness strategies. The authors proposed that companies should have internal auditors whose duties would be to assess state of cybercrime protection within a company and provide council on how to improve cybercrime defence.

Almadhoob and Valverde (2014) also explored how the issue of cybercrime in organisations can be tackled via the addition of cyber security within companies. The authors state that following the events of the Arab Spring in 2011, the Kingdom of Bahrain suffered increasing rates of cybercrimes that should be addressed. The authors again noted that the most popular cybercrimes were viruses sent in emails to gain access to a computer within an organisation, or a DDoS attack, and studied how prepared and informed the IT departments of major organisations in the Kingdom of Bahrain were. The authors concluded their study by suggesting that official discussions on the matter of cyber-security within organizations with a purpose to inform those in charge, as well as employees, of the most contemporary threats and security measures would help reduce cybercrime rates. It must be noted, however, that the authors were not able to collect large a sample of data, as the Kingdom of Bahrain has limited resources and settled with a sample number of 34 organisations.

Moving on, Leppanen and Kankaanranta (2017) explored cybercrime investigation within the police force in Finland. The authors state that in the last few years, law enforcement in Finland has focused heavily on improving cybercrime prevention, participating in different cyber training programs through a partnership with the Nordic Computer Forensics Investigators. The article provides a thorough discussion on how forensic cybercrime investigative processes work within the police, how cybercrime investigation training is conducted and how it could be improved. The main aim of the article was to show another form of cybercrime prevention – namely computer forensic investigation. Me and Spagnoletti (2005) discussed practical implications of computer forensic investigation in a case study of an online pedo-pornography

investigation. Firstly, the authors reviewed the issue of the online pedo-pornography from a perspective of situational crime prevention, then discussed how investigative processes could be improved from a technological point of view. Murashbekov (2015) reviewed the topic of cybercrime prevention in developing countries and ways it could be improved. He compared the way cybercrime is being addressed in the Republic of Kazakhstan to that in Western countries. The author states that cybercrime rates in the Republic of Kazakhstan are lower in comparison to the EU or U.S., because Western countries emphasise different prevention tactics, methods and strategies, while Russia is focused on fighting cybercrime from a legislative perspective. Murashbekov argues that cybercrime should be tackled by law enforcement and cyber-security specialists, however, the research shows that different technical methods of protection also proved to be successful. Rashkovski, Naumovski and Naumovski (2015) also produced a study where they explored the effectiveness of different cybercrime prevention from legislative as well as general approaches in the former Yugoslav Republic of Macedonia. The authors discuss different articles of the Criminal Code of Macedonia that specifically address cybercrime and argue that some of the most effective ones could be implemented on an international level. The academics believe that the situation in Macedonia is proof that cybercrime could be tackled from a legislative point of view and give recommendations to international organisations to explore the legislation of Macedonia on a matter of cybercrime prevention.

Harris and Singla (2014) studied the impact of cybercrime on the economy of Ireland and estimated the impact to €630 million. The authors explored the risks and threats of cybercrime from the perspective of the economy, how cybercrime affects the state of the economy and how to negate risks from an economy point of view. Harris and Singla explored government investments in cybersecurity and correlation to the effectiveness and concluded that if the government invested more money in cybersecurity, it could reduce cybercrime damage, subsequently saving money. Furthermore, the article raises the point of awareness and how crucial it is to the business and government environment. Another contemporary primary prevention technique was employed by the University of Central Arkansas in late 2017 (Anonymous, 2017). The university has built a so-called ‘cyber-range’ where students can experience cyber-attacks simulated by a computer in real time to learn and explore different cybercrime prevention methods. Furthermore, a new bachelor’s degree course in cybersecurity starts in the fall of 2018. The governor of Arkansas believes that the cybercrime threat is real and emphasized the importance of education related to computer sciences.

As stated before, different countries address cybercrime from different perspectives, yet some countries recognise cybercrime as being an international issue and are trying to contribute to cybercrime prevention on an international level. Li (2007) discussed cybercrime as an international issue and how the problem of cybercrime could be balanced in the world. He stated that some international organisations have already taken steps towards the discussion of the cybercrime matter – for instance, the United Nations Crime and Justice Information Network (United Nations Crime and Justice Information Network, 1999) and Police Commissioners’ Conference Electronic Crime Working Party (2000). The author further discusses specific amendments in legislations made by professional international crime policing organisations such as Interpol, The Council of Europe (COE), The Group of Eight (G8),

The United Nations (UN) and others. He concludes that many different legislative adjustments in relation to cybercrime were already made, however many gaps in laws on an international level still exist. Li also discusses that some major organisations, such as the UN, should be making more of an impact, as they have more influence.

Other academics explored the most recent technological inventions and how they could be used in the cybercrime prevention field. Mills and Byun (2006) discussed biometrics when it was just introduced, and suggested ways they could be used to protect consumers. The authors explain that biometric protection in a form of a fingerprint scan, iris scan, voice or face recognition could add another layer of protection to personal electronic devices. They argue that by employing such technologies in cybersecurity, cybercrime rates could be exponentially reduced. Years later, Frost and Sullivan (2014) also analysed biometric technologies on the consumer market and concluded that fingerprint biometrics will be dominant in the future. Nowadays, most modern smartphones have at least one biometric recognition technology, such as fingerprint, iris scan, or face and voice recognition. Maher (2017) went even further and explored how artificial intelligence (AI) could help in fighting cybercrime. Academics discussed technologies such as machine learning, deep learning and User and Entity Behavior Analytics (UEBA). UEBA technology could be used for threat detection by analysing network activities and identifying malicious behaviour, then reporting it to a human operator. UEBA can be taught the patterns of normal network behaviour and, through an algorithm, learn to detect any deviances; the author states that UEBA provides close to 100% report of accuracy.

To conclude, the cybercrime threat is very real and many people around the world are concerned about being exposed to different cybercrimes. As such, it is being recognised and addressed by criminologists and different private and governmental as well as international organisations. Cybercrime prevention is moving forward, developing alongside the technological progress. In the 'Analysis' section further in the paper, a study of whether people of different age groups use personal electronic devices more, if people are getting more exposed to cybercrimes and if the use of prevention mechanisms increases as well will be presented in detail. Consequently, concluding whether the rates of use of personal electronic devices and exposure to cybercrime have positive correlations with the use of prevention mechanisms, or whether the issue of cybercrime evolves and cybercrime prevention should be addressed more seriously.

RESEARCH QUESTIONS

Following the section above, it was determined to explore three main sections of interest that will assist understanding of which factors shape victimisation and consequent use of prevention measures online.

- Changes in trends of cyberspace in England and Wales
    - How has the number of internet users has changed over the years?
    - Do people use the internet more often?

- Subsequently, if people are more exposed to a cyber environment, are they more worried about being victims of cybercrime?

The main objective of this section is to shed light on the 'Internet era', using an example of the general population of England and Wales. Key questions aim to find if the internet does indeed play a major role in daily human lives, if more and more people use internet daily, several times a day over the years and if people truly are more concerned about being victimised online. The number of studies that are aimed at exploring current trends in the cyber environment and especially use of the internet are very limited. Therefore, it would be beneficial to address such gap and explore trends in the internet specifically. The literature review explored PEDs and their direct relationship to the internet. Furthermore, Baker (2013) stated that 76% of survey respondents were worried about being victims of cybercrime, however it was not explored whether worry of cybercrime and exposure to cyber environments are related.

- Understanding of current state of victimisation and use of prevention measures in cyberspace in England and Wales
  - What is a current trend of cybercrime victimisation in a cyberspace for the general population?
  - Do people use more prevention measures and are they effective?

Currently there are many different opinions on the current state of cyberspace victimisation and accurate cybercrime victimisation statistics are not that accessible, particularly for England and Wales. In this section, actual victimisation rates online and changes in victimisation rates online over the years are going to be discussed, as well as use of different prevention measures and their consequent effectiveness.

- Different factors that could possibly affect victimisation rates in cyberspace
  - Are individuals who are more worried about cybercrime more likely to be victimised in cyberspace?
  - Does age of the victim affect victimisation online?
  - What other variables could be important when explaining victimisation rates online?

If individuals are worried about cybercrime, do they understand the threat and subsequently use prevention measures more responsibly, thus decreasing the number of victimisation cases? Or, do individuals that are more worried about being victimised online behave more 'desperately' and thoughtlessly 'overprotect' themselves, falling into obvious traps when advertised 'prevention measures' are actually malwares themselves. Another important variable to consider is the age of a typical internet user. As different generations encountered the internet at different points in their lives, younger people are likely to be more comfortable using the internet, as they were born and grown up interacting with internet technologies, while older people were likely to be introduced to them when they were already mature. Furthermore, other factors included in CSEW should be explored to understand what else might be crucial to consider when exploring above-mentioned topics. CSEW is a general crime victimisation survey conducted in England and Wales but the present study is aimed at a

specific type of crime which is considered to be a global phenomenon. Nonetheless, CSEW is the most comprehensive and professionally conducted study available that considers cybercrime. Considering above-mentioned limitations, analyses of this particular study are not aimed at determining a clear connection between different factors, but rather to explore cyberspace in England and Wales and provide an overview of the current state of cybercrime.

In order to explore changes in cyberspace trends in England and Wales, firstly, descriptive analyses are going to be carried out to establish actual data as reported by the survey respondents. Analyses such as level of worry of being victimised online, use of the internet, frequency of internet use, self-reported number of victimisations and number of prevention measures used online. It will assist in understanding the actual state of cyberspace, making it clear how many people actually use the internet and how often, how many people are afraid of becoming cybercrime victims and how many people are actually getting victimised online and, moreover, what they do to protect themselves online. Secondly, in a cross-variable analyses section, relationships between different variables are going to be outlined. Variable combinations such as worry level and victimisation, worry level and use of prevention measures, victimisation and age, prevention measure use and age are going to be analysed with alongside each other to determine a relationship between these variables. This method of analysis will summarise variables that have significant relationship between each other. The final part of the analyses section is going to include regression tables that display the same factors as in the cross-variable section or other factors included in CSEW to summarise which factors are most significant to study when analysing victimisation or use of prevention measures online.

Exploring these three subtopics, it is going to be concluded whether the general population does actually use the internet more, whether cyberspace is becoming safer as people adapt to the cyber environment and address cyber threats more effectively, consequently outlining areas that could be explored more thoroughly for more in-depth understanding of how exactly different factors affect cyberspace.

METHODOLOGY

The main objective of the research is to explore the trends over time and to observe the cross relationships between use of internet technology, fear and exposure to cybercrime and use of security measures, making quantitative methodology an obvious choice for this project. According to Neuman (2002), quantitative research methods should be used when research questions are focused on a large group of people, therefore making it possible to apply research findings to a general population. Moreover, one of the research aims was to establish if rates of internet use, cyberspace victimisation and use of cybercrime prevention measures change over time, meaning that numerical data is necessary to meet that goal. Babbie (2010) stated that if the research goals can be met by gathering numerical data with a purpose of generalising it across different groups of people or explaining a particular phenomenon then quantitative research methods should be employed.

The objectivist paradigm is an ontological stance for quantitative research that defines social phenomena as something constructed by external factors and not influenced by researchers (Tuli, 2011). Furthermore, the positivist paradigm is an epistemological stance for quantitative research. It defines the world as an objective reality and should be observed by a researcher as such. When conducting quantitative research, it is crucial to understand that the social world should be perceived as an objective reality, not subjective vision, and moreover, realise that any studied social phenomenon is not shaped by an individual but by an external factor. Applying these concepts in respect to the study, while cybercrime has been discussed as a fluid phenomenon and a complex issue, for a quantitative project to take place the concepts of internet use, fear of crime, exposure to cybercrime and other aspects of the study will be operationalised in line with data available on the topic. However, the qualitative approach would be especially advantageous if it was decided to study behaviour of certain individuals from different age groups. For example, to explore the reasons behind people using more prevention measures when they are more worried of cybercrime and what these measures exactly are; whether they are actually downloading malwares that are hidden behind advertised “anti-malware tools” or if there are other reasons behind it.

The statistical data used in this research comes from the secondary data set Crime Survey for England and Wales (CSEW), which is the most sizable and extensive source of statistical data for reported victimisation rates in England and Wales. Firstly, CSEW data collection began in 1982, thus it is possible to track changes in trends of victimisation rates for the last 36 years, however questions related to this particular study did not appear in earlier editions of CSEW. Questions about particular types of cybercrime victimisation started to appear as early as 2011. Secondly, the survey provides a statistically ambitious sample size of more than 30,000 households interviewed each year which would be a difficult-to-impossible task to achieve conducting one’s own quantitative research with realistic timing and financial constraints. Moreover, the Office for National Statistics (ONS) who conduct the CSEW are able to select random addresses from the Royal Mail’s list of addresses. Sampling of the survey is not exactly random, but ‘stratified random’ and ‘semi-clustered’, subsequently ensuring that people of all genders, ages and social backgrounds are considered in the survey and it also allows the possibility to generalise findings of the study and reflect these findings to a whole nation.

As mentioned, the Crime Survey for England and Wales is targeting households, meaning that businesses and organisations, homeless people and prisoners and young people living in student dorms are absent from the sample. However, businesses and organisations are not the interest of this particular study because the aim of the research is to explore the public, not enterprises. Cybercrime research where businesses are of interest would require a different theoretical approach due to concepts of fear of cybercrime and use of prevention mechanisms coming from a perspective of financial considerations. Furthermore, in some cases, businesses and organisations are targeted for different reasons to individuals, are more educated about cyber threats having their own specialists responsible for cyber security and so that data would undermine the key aims of this study. Institutionalized people and prisoners are less likely to freely use computers and internet in line with the general public to be of the interest of this study. On the other hand, students in dorms who are absent from the data set would broaden the research as one of the studied age groups are young people

aged from 16 to 25. An important factor to note is that the Crime Survey of England and Wales is a victimisation survey conducted post-factum and explores previous year victimisations of the respondent, which is advantageous in comparison to police-provided reported crime data because it eliminates the factor of crimes that were not reported. This is particularly meaningful when exploring an issue such as cybercrime because of cybercrime being relatively a new and fluid type of crime and people still not knowing where, how and why cybercrime should be reported (Bidgoli & Grossklags, 2016).

However, the Crime Survey for England and Wales is not flawless and proposed several challenges while conducting a research. First, as mentioned earlier, the CSEW is a household survey that does not cover organisations. In a matter such as cybercrime, attacks on organisations and attacks on individuals are completely different cases, however both are equally important in understanding trends in contemporary cyber environment. Consequently, this study only represents trends of cyberspace in relation to attacks on individuals. Secondly, questions in the CSEW about cybercrime tend to change over the years, expanding answer options for the respondents making it difficult to track changes over the years. Moreover, the CSEW is not a cybercrime focused survey and often does not provide details necessary to explore certain subtopics. On the other hand, as cybercrime is a very fluid issue that is not yet established and formed as a crime and tends to change very often it is a positive development that CSEW is adapting to these changes. The third and most confusing issue that was encountered during the research is that in recent years of CSEW different respondents were asked to answer different cybercrime related questions. For example, respondents who answered the question 'how worried are you about being victimised online' did not answer any questions related to prevention measures used online making it impossible to track a relationship between 'worry of cybercrime' and 'use of prevention measures online' for year 2016.

For the analyses, where it was required to make comparisons between different ages, respondents were categorised by age groups: young (ages 16-25), middle (ages 26-45) and old (ages 46-100). These particular age groups reflect how marketers within the technology field categorise audiences: generations X, Y, Z (Williams & Page, 2011). Generation X (aged 45+ in 2017), who were born in 1970s when computers were firstly introduced. Generation Y (aged 35+ in 2017) who were born 1980s when technologies got more common and internet was getting developed, and generation Z or Millennials (aged 16+ in 2017) who were born in mid-1990s to mid-2000s and were comfortable with computers, smartphones, internet since a young age. The fourth issue, recoding of data set was conducted because of different sections of the survey being coded differently. In section 'experience of cybercrime', variable '0' was equalled to answer 'No', but in section 'prevention measures used', variable '0 = Yes', which required picking all relevant questions and recoding them in a data set where same variables were responsible for same answer in every question. Even though the data set required some recoding, it was logically structured with smooth transitions from sections such as demographic factors and use of internet to worry about being victimised online and prevention measures used, which is very convenient for the study.

ANALYSES

Descriptive analyses:

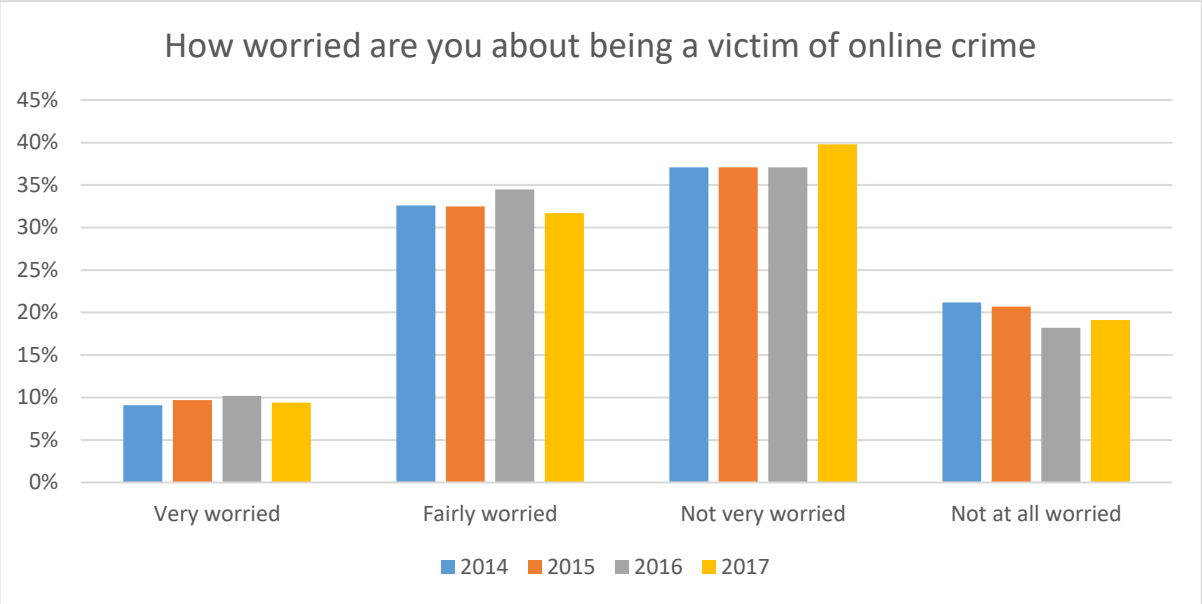


Figure 1. How worried are you about being a victim of online crime, CSEW 2014-2017.

	2014	2015	2016	2017
N	7216	6858	7375	7557
Mean (Std. error)	1.7 (.011)	1.69 (.011)	1.63 (.010)	1.69 (.010)
Very worried	9.1%	9.7%	10.2%	9.4%
Fairly worried	32.6%	32.5%	34.5%	31.7%
Not very worried	37.1%	37.1%	37.1%	39.8%
Not at all worried	21.2%	20.7%	18.2%	19.1%

Table 1. How worried are you about being a victim of online crime, CSEW 2014-2017.

In order to explore trends in worry of cybercrime, a factor found to be important in the study conducted in 2013 by Baker, CSEW respondents' levels of worry were compared between years 2014 and 2017. Percentage values of responses underpin that overall number of respondents who are not worried about being a victim of cybercrime was lowering from years 2014 (21.2%) to 2016 (19.1%). Considering that, the number of 'very worried' respondents was increasing in the period of 2014-2016 from 9.1% to 10.2% and then lowered to 9.4% in 2017; the graph 'very worried' accurately represents change in worry levels of being a victim of cybercrime across a 4-year period. Moreover, the majority of the responses are concentrated in the middle (fairly worried, not very worried) and less respondents chose to answer 'extremes'. It can be assumed that people tend to pick less 'precise' options because they are not sure how they should feel about being victims of cybercrime as a consequence of not being educated enough on the current state of cybercrime, however to confirm such assumptions a qualitative approach would be required.

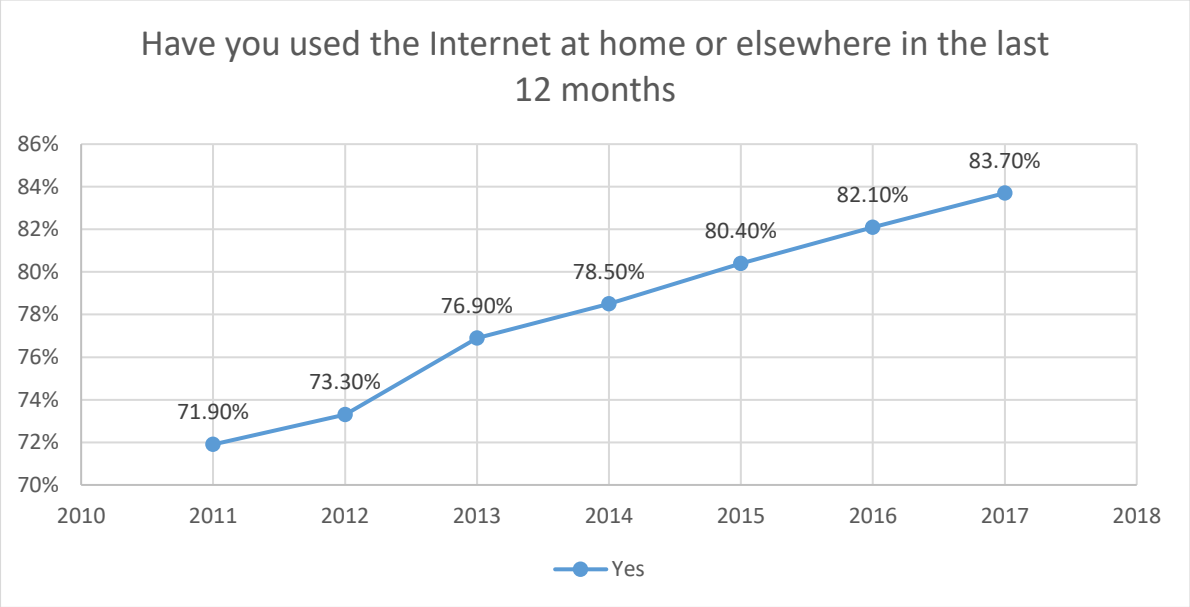


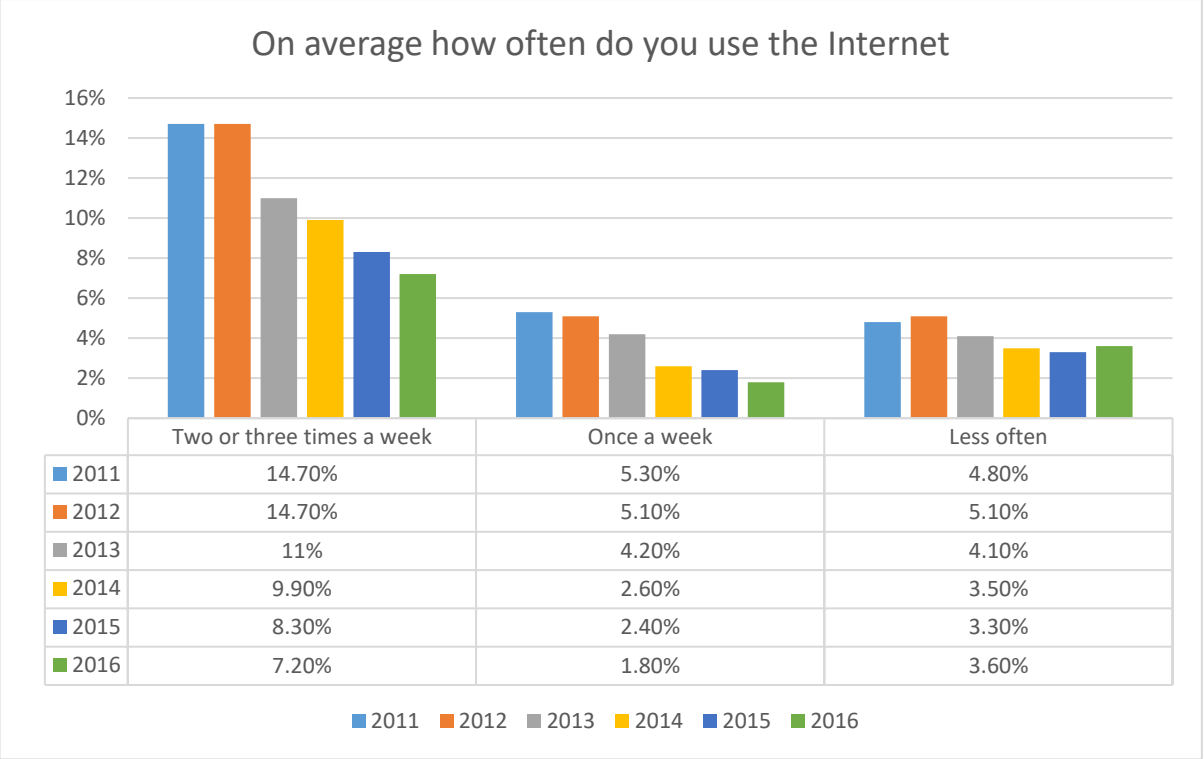
Figure 2. Have you used the Internet at home or elsewhere in the last 12 months, CSEW 2011-2017.

Data on use of the internet in the last 12 months is an important variable for the study as it allows narrowing down sample size to people who have used the internet, shifting the focus of the study on to people who have actually used the internet. Figure 2 shows how the number of internet users has increased over the 7-year period from 2011 to 2017. In year 2011, 71.9% of 11,666 respondents have used the internet and in year 2017, that number increased to 83.7% of 35,417 respondents. Hernandez-Castro and Boiten (2014) who explored the prevalence of cybercrime in the UK had also stated that almost 80% of the residents of the UK had internet connection in 2014.

	2011	2012	2013	2014	2015	2016	2017
Yes	71.9%	73.3%	76.9%	78.5%	80.4%	82.1%	83.7%
No	28.1%	26.7%	23.1%	21.5%	19.6%	17.9%	16.3%
N	11666	11421	8080	8381	7884	26817	35417

Table 2. Have you used the Internet at home or elsewhere in the last 12 months, CSEW 2011-2017.

Analysing values of Table 2, it can be concluded that the number of internet users is increasing for approximately 2% each year with a spike of 3.6% increase in year 2013. That spike can be explained by fibre optic broadband becoming more available. The Office for National Statistics (2013) compared how many households in the UK were connected to the internet between years 2012 and 2013. They found that broadband connection over Digital Subscriber Line (DSL) had dropped by 12% and connection by fibre optic broadband had increased 12%. Arguably, faster and more reliable fibre optic broadband had influenced the more than average increase in use of the internet in 2013. It is possible that in the next 8 years, the number of people who would have used internet in the last 12 months will be close to 100%.



	Two or three times a week	Once a week	Less often
2011	14.70%	5.30%	4.80%
2012	14.70%	5.10%	5.10%
2013	11%	4.20%	4.10%
2014	9.90%	2.60%	3.50%
2015	8.30%	2.40%	3.30%
2016	7.20%	1.80%	3.60%

Figure 3. On average how often do you use the Internet, CSEW 2011-2016.

Bomhold (2013) and Phelps *et al*. (2017) who analysed use of smartphones for different academic purposes by students concluded that up to 97% of students use smartphones for different academic and non-academic internet related purposes throughout the day. Exploring how tendency of internet use changes over time makes it possible to draw a conclusion further in the research based on that data. It can be seen that in general, the number of people who are using internet several times a day is increasing and the number of people who use the internet occasionally is in decline. After 6 years, the number of people who used internet several times a day increased by 12.1%, the number of people who used internet two or three times a week decreased by 7.5%, the number people who used the internet once a week decreased by 3.5% and the number of people who used the internet less often than once a week decreased by 1.2%.

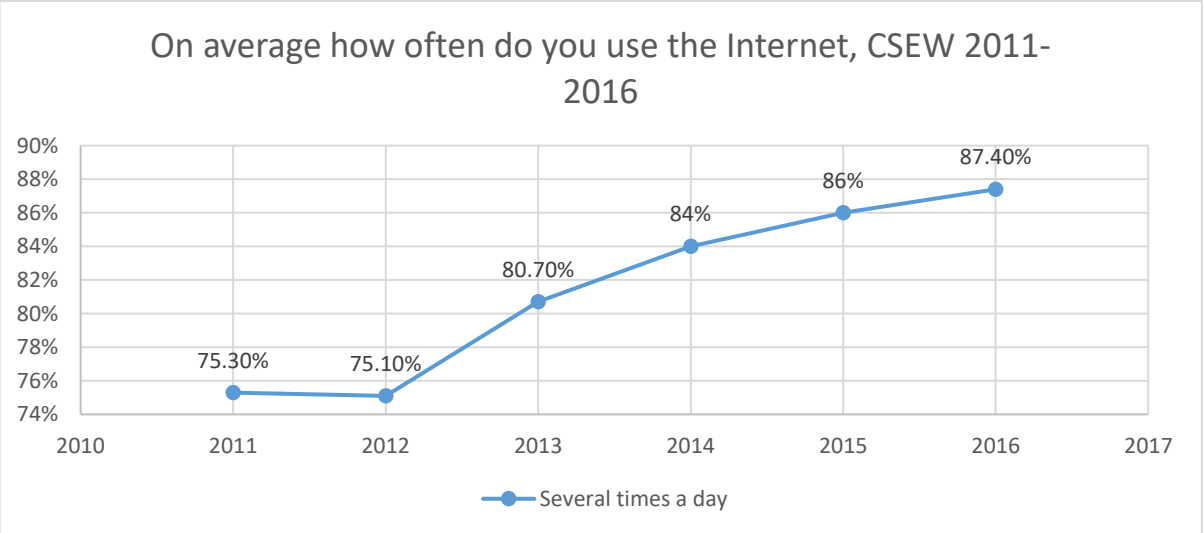


Figure 4. On average how often do you use the Internet, CSEW 2011-2016.

Figure 4 provides a closer look on how the number of people who used the internet several times a day changed over years. In year 2012, the number slightly decreased by 0.2%, however the year after it had increased by 5.6% and was increasing by approximately 2% in the following years. Overall, number of people who used the internet less often than several times a day was steadily decreasing and number of people who used the internet several times a day was increasing. It can be argued that respondents were changing their response from less often to several times a day over the years because new opportunities within the internet arise, such as online banking, music and media streaming services, social medias making people use internet more often for a range of different activities. People spend more and more time in the internet environment because almost everything is accessible there: jobs, business, leisure, shopping and others (Svingstedt, 2017).

	2011	2012	2013	2014	2015	2016	2017
0	65.1%	66%	70.8%	70.7%	72.9%	76.5%	78.1%
1	30%	28.8%	24.2%	24.4%	23.1%	20%	18.1%
2	4.2%	4.4%	4.1%	4.2%	3.3%	2.9%	3%
3	0.7%	0.8%	0.9%	0.6%	0.6%	0.5%	0.6%
4	0.1%	0.1%	0.1%	0%	0.1%	0.1%	0.1%
TOTAL1+	34.9%	34%	29.2%	29.3%	27.1%	23.5%	21.9%
TOTAL2+	4.9%	5.3%	5%	4.8%	4%	3.5%	3.8%

Table 3. Total number of victimisations, CSEW 2011-2017.

Hernandez-Castro and Boiten (2014) have analysed the CSEW for 2011/2012 and found that 37% of internet users were victimised, which in the case of this particular study is 34.9% for 2011 and 34% for 2012. Nonetheless, analyses provided by the academics only analyse a single CSEW sweep. Row "0" of Table 3 shows that 65.1% of respondents were not victimised in 2011 and in 2017 that number increased to 78.1%, which means that over 7 years 13% less people experienced cybercrime. The number of people who have experienced a single event of cybercrime was also decreasing over that period. In 2011, the percentage of people who had experienced cybercrime once was at 30% and in 2017 that number decreased to 18.1%, meaning an 11.9% decrease of the number of respondents who were victimised just once. Row "TOTAL1+" summarises the rest of the respondents who were victimised at least once and decreased from 34.9% in 2011 to 21.9% in 2017.

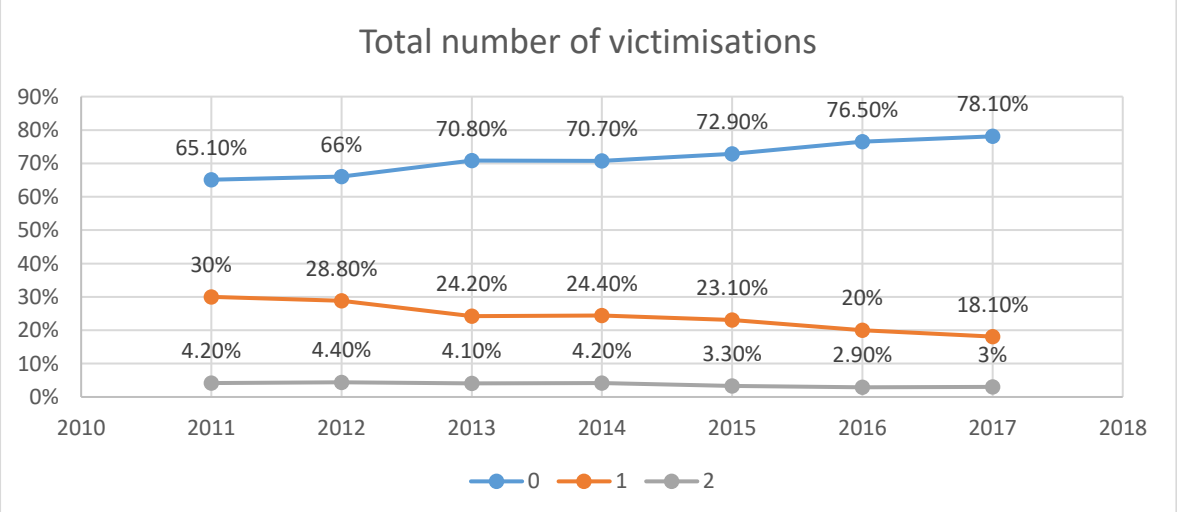


Figure 5. Total number of victimisations, CSEW 2011-2017.

A visual representation of victimisation between years 2011 and 2017 clearly shows that the overall number of victimisations has dropped in the 7-year period. The percentage of respondents who were not victimised at all is steadily increasing and on the other hand, the percentage of respondents who were victimised once is steadily decreasing. Nonetheless, the percentage of respondents who were victimised twice or more is also decreasing but at a slower pace. It can be concluded that the overall number of victimisation has reduced for people who were victimised once, however the change for people who are inclined to suffer repeat victimisation is less significant.

	2011	2012	2013	2014	2015	2016	2017
Mean (Std. error)	.4 (.007)	.4 (.007)	.35 (.008)	.35 (.007)	.32 (.007)	.28 (.005)	.27 (.004)
N	8383	8376	6216	6583	6338	11167	15277
Std.Deviation	.614	.62	.608	.593	.56	.543	.555
Variance	.377	.384	.370	.351	.331	.295	.308

Table 4. Average number of victimisations, CSEW 2011-2017.

On the Table 4 row, 'Mean' shows average number of victimisations over the years. In years 2011 (0.4) and 2012 (0.4) the number remained unchanged, then lowered to 0.35 in years 2013 and 2014 and then started to drop more notably until the average number of victimisations of 0.27 in year 2017. It can also be noted that the standard deviation and variance are also dropping, meaning that the gap between the average number of victimisations per household is less; less households are victimised multiple times or victimised an extreme number of times (such as 10) and households are closer to each other on average.

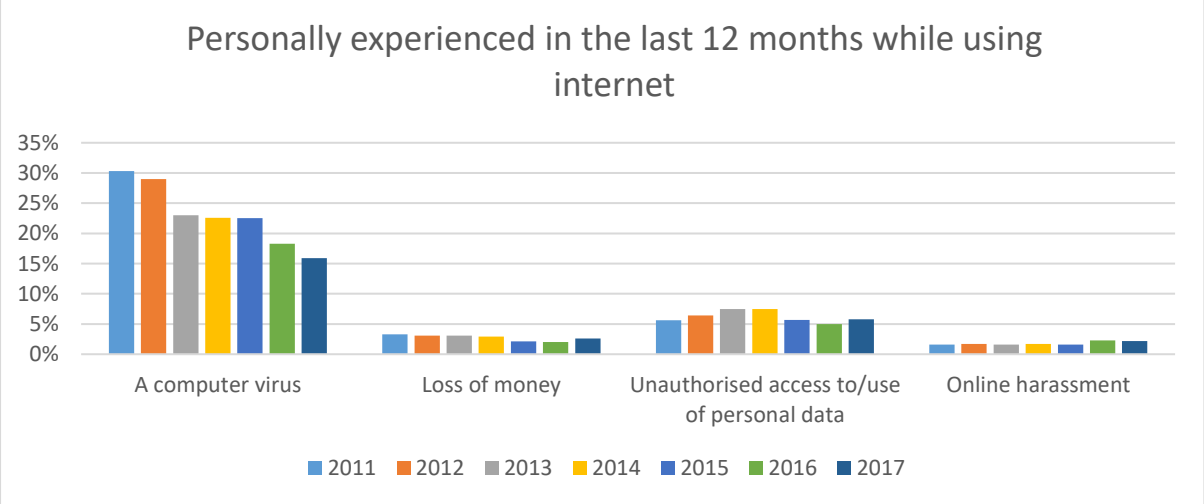


Figure 6. Personally experienced in the last 12 months while using internet,

CSEW 2011-2017.

The first type of cybercrime taken into consideration is a 'Computer Virus', which dropped by approximately 15% in the period of 7 years. It is the most popular type of cybercrime amongst the four cybercrimes introduced in the figure. Such a decrease in computer virus cybercrime

likely was a consequence of an introduction of an in-built Microsoft antivirus in the common Operating System (OS) Windows Microsoft. The number of 'Loss of money' incidents remained almost unchanged with a slight decrease in years 2015 and 2016 and then slight increase in 2017. Such a pattern could be explained by a 'mobile banking' technology introduction, and when cyber criminals have adapted to that technology, rates have increased again. On the other hand, 'Unauthorised access to/use of personal data' cybercrime was increasing from year 2011 to 2014 then started to drop until year 2016 and then again increased in 2017. 'Online harassment' types of offence rates almost remained unchanged from 2011 to 2015 and then increased by 0.7% in 2016. Saying that, it can be argued that represented choice of cybercrimes is limited because many of the contemporary cybercrimes might not fit within these four categories making this figure not representative for other cybercrime categories.

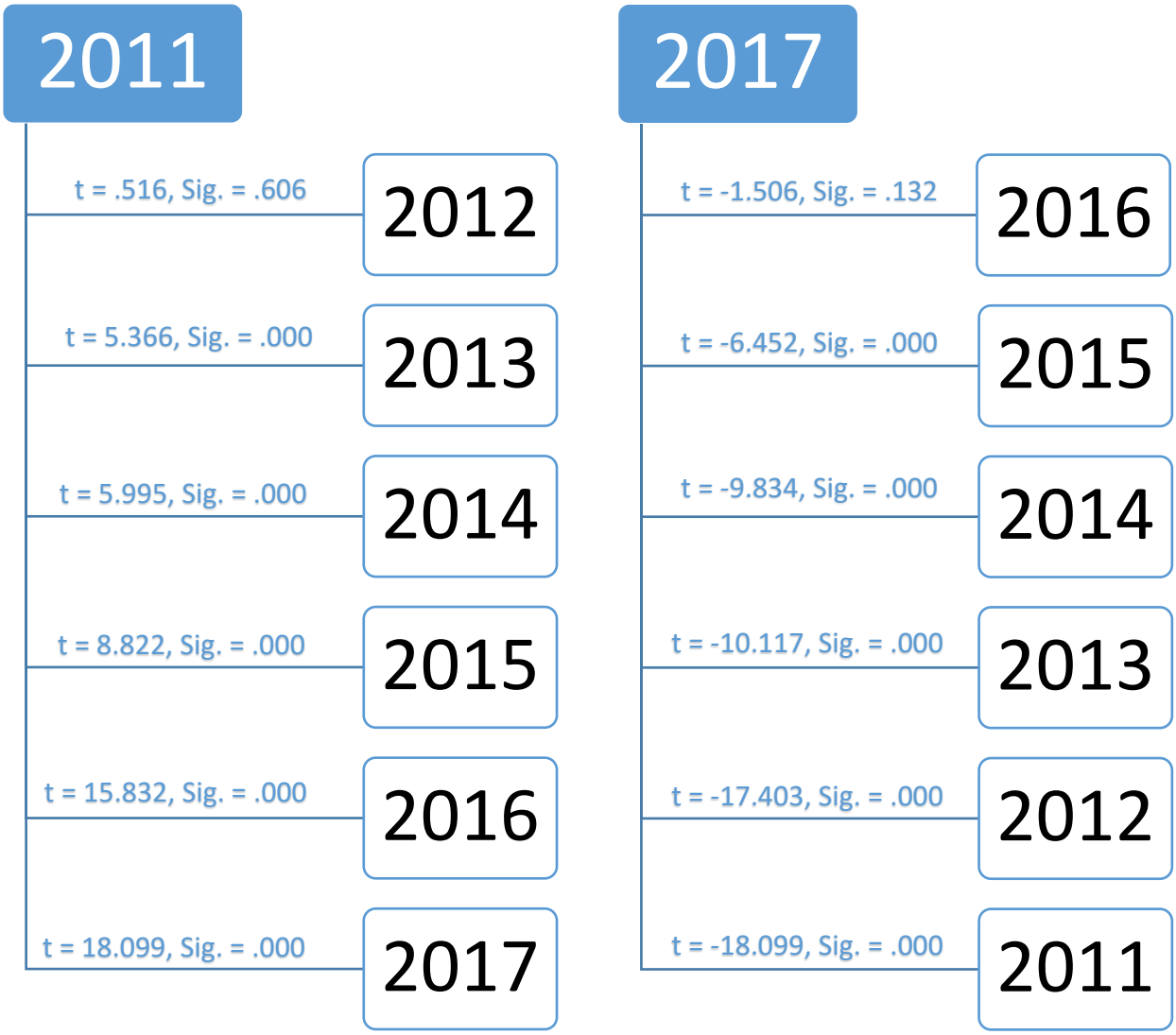


Figure 7. Significance of number of victimisations in different years, CSEW 2011-2017.

Exploring the number of victimisations significance in year 2011 to the following years until 2017 and then in reverse significance of year 2017 to previous years until 2011, it can be seen that the change in years 2011 to 2012 is not significant ($p > .05$; $p = .606$), however change compared to year 2013 and all the following years is significant ($p < .05$). The same pattern can be noted in the reverse figure; year 2017 is not significant (sig > .05; sig = .132) to year 2016, however is significant to 2015 and all the rest (sig < .05). Furthermore, a higher gap between years leads to higher '*t*' value meaning that further years show more important difference to the original year, underpinning the above-mentioned steadily decrease in victimisation.

	2014	2015	2016	2017
0 prevention measures	7.6%	15.6%	17%	16%
1 prevention measure	15.4%	14.5%	14.1%	12.8%
2 prevention measures	17%	17.9%	18.4%	17.9%
3 prevention measures	24.8%	22.8%	22.4%	24.4%
4 prevention measures	35.3%	29.2%	28.2%	29.9%

Table 5. Number of prevention measures used, CSEW 2014-2017.

Analysing the number of prevention measures would not be particularly meaningful on its own, however providing this type of descriptive statistics will allow for a further cross-variable worry level/number of prevention measures analyses. The first row of the table displays that in 2014 just 7.6% of respondents have not used any prevention measures and in 2015 that number increased to 15.6%, then in 2016 increased to 17% and in 2017 dropped to 16%. The percentage of respondents who used one prevention measure dropped from 15.4% in 2014 to 12.8% in 2017. The percentage of respondents who used two or three prevention measures remained almost the same across the 4-year period, however the percentage of respondents who used 4 prevention measures dropped from 35.3% to 29.9%.

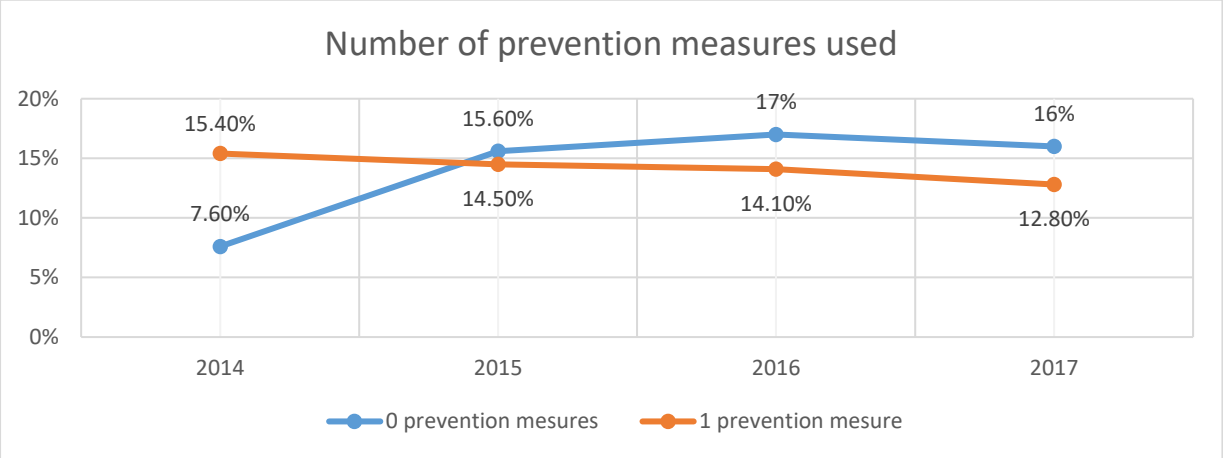


Figure 8. Number of prevention measures used, CSEW 2014-2017.

Figure 8 visually represents the first and second rows of Table 5, showing a decline in use of prevention mechanisms. The percentage of respondents who reported 0 prevention measures used has more than doubled in the 4-year period. Moreover, rates of people who used one or more prevention measures dropped, meaning that people in 2017 use less prevention measures than in 2014. The trend in overall decline of use of prevention measures can be explained by introduction of in-built prevention measures. Such as in-built antivirus discussed earlier, two-factor authentications that are getting more common, fingerprint scanners on mobile devices or internet payments secured by SSL certificate becoming obligatory.

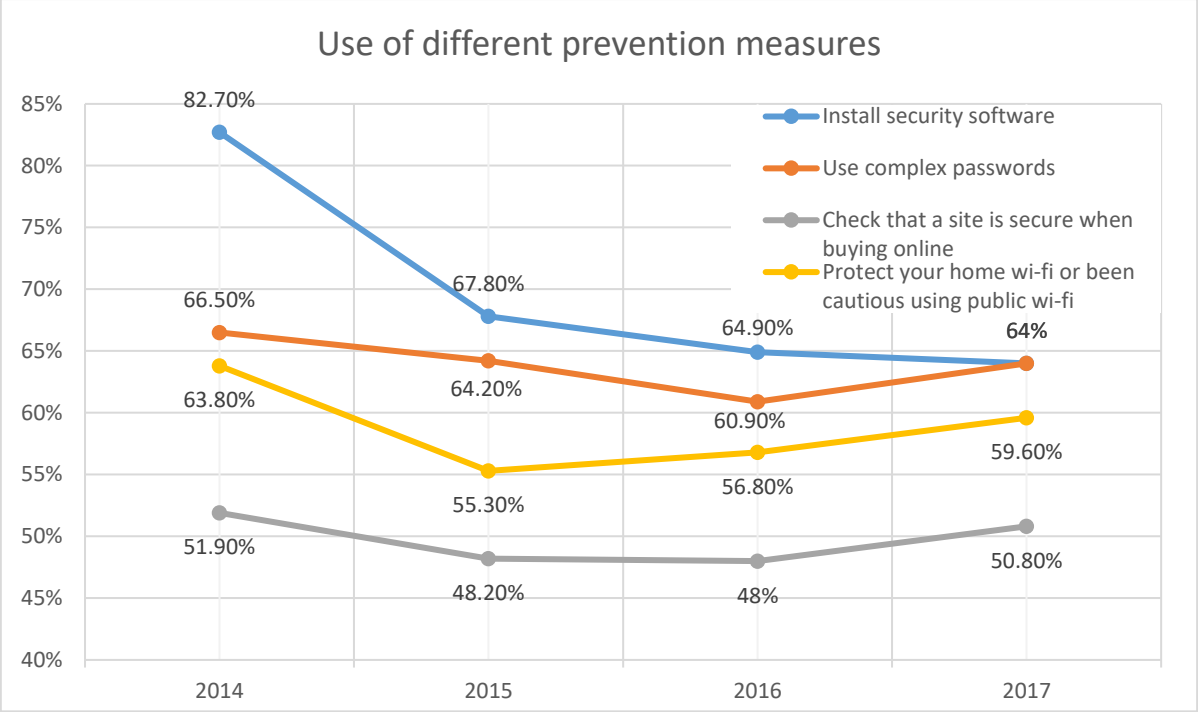


Figure 9. Use of different prevention measures, CSEW 2014-2017.

The figure of trends in use of particular prevention measures stands as a representative example for change in trends of overall use of prevention measures. The first is 'Install security software', prevention measure which is mainly aimed at preventing 'computer virus' crime has dropped from 82.7% to 64%, as well as discussed earlier in Figure 6 'computer virus' cybercrime rates were dropping. The reason for security software being installed less often is the same, introduction of inbuilt security measures in most popular OS (Operating System) Microsoft Windows. The other three prevention measures show a slight decrease from 2014 to 2016, however in year 2017 all three show an increase. However, the figure cannot be used in explaining overall trends in use of prevention measures as it only includes 4 prevention measures that are not ubiquitous.

	2011	2014	2017
Only download known files or programs	-	-	53.8%
Only used well-known or trusted sites	66%	-	58.6%
Download software updates and patches whenever prompted	-	49.5%	42.4%
Used complex passwords	-	66.5%	64%
Used a different password for each different online account	-	42.2%	38.9%
Checked for signs that a site is secure before buying goods	-	51.9%	50.8%
Deleted suspicious e-mails without opening them	-	70.8%	73.7%

Logged out of websites when you are finished	-	66.9%	58.8%
Adjusted website account settings (e.g. privacy)	-	-	29%
Installed anti-virus or other security software such as firewall	66.5%	82.7%	64%
Scanned computer regularly for viruses or other malicious software	-	-	47.7%
Protected your home wireless connection (Wi-Fi) with a password or been cautious using public Wi-Fi	-	63.8%	59.6%
Only added known persons as friend on social networks	-	-	53.9%
Been careful about putting personal details on social networking sites	-	-	62.4%
Only use credit cards (not debit/charge cards)	27.8%	23%	-

Table 6. List of questions in questionnaires related to cybercrime, CSEW 2011,2014,2017.

Justifying the choice of certain prevention measures and comparison between years 2014 and 2017 in Figure 9, it can be seen in Table 6 that in year 2011 it was just 3 questions about security in cyberspace, then in 2014 the number increased to 8 questions and in 2017 it was 14 questions. Saying that, it would be impossible to compare use of prevention measures such as 'scanning computer regularly' as this question was just introduced in 2017. As new threats and countermeasures emerged, lists of questions were expanding, giving respondents more options and opening possibilities for more in-depth analysis. For example, looking at data provided on a question 'Installed anti-virus or other security software such as firewall' it can be noted that number of respondents who answered that question has increased by almost 20% from 2011 to 2014 and then again dropped by almost 20% from 2014 to 2017. Considering Figure 6 that represented rates of virus type of cybercrime experience number of victimised respondents was around 30% in 2011 and in 2014 it dropped to 22% when more respondents chose to answer 'installed anti-virus' and then in 2017 it dropped to 16%, however, less respondents installed anti-virus software. The data provided in Table 6 also supports an 'in-built anti-virus' argument, however, the main purpose of the table is to show how the list of prevention measures has expanded over the years.

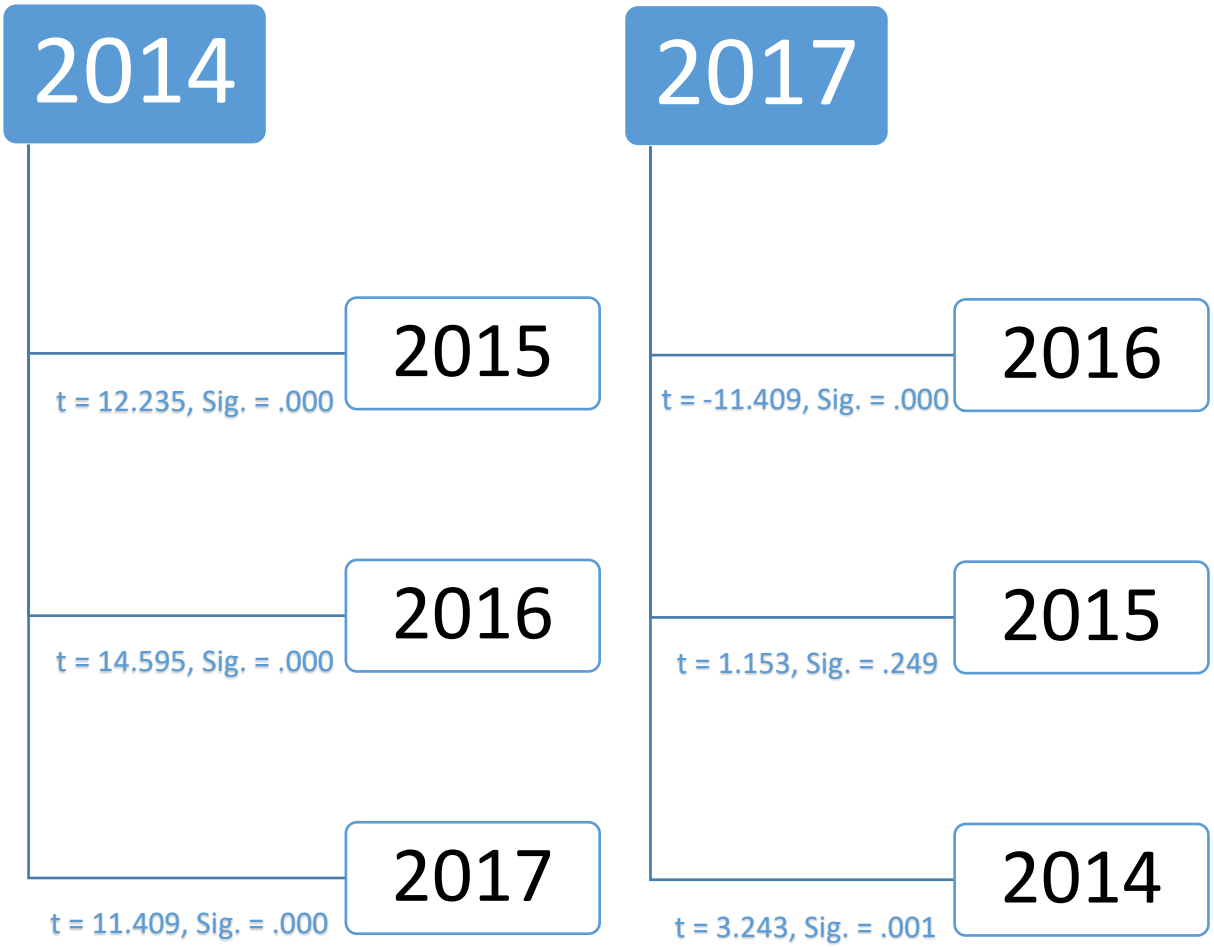


Figure 10. Significance of number of prevention measures used in different years, CSEW 2014-2017.

	Mean (Std. error)
2014	2.65(.0161)
2015	2.36(.0179)
2016	2.31(.0170)
2017	2.38(.0167)

Table 7. Average number of prevention measures used in different years, CSEW 2014-2017.

Defining averages for prevention measures used in different years is to confirm overall trends and allows an opportunity for a cross-variable analyses later in the cross-variable section. In 2014, respondents used 2.65 prevention measures on average then in 2015, number has dropped to 2.36, in 2016 dropped by another 0.05 and in 2017 it has increased back to 2.38 prevention measures on average per respondent. Figure 6 represents significance between these changes. Changes when comparing year 2014 to other years are all significant ($p = .000$; $p < 0.05$), however when comparing 2017 to other years it is only significant when looking at 2017 to 2016 ($p = .000$; $p < 0.05$) and 2017 to 2014 ($p = .001$; $p < 0.05$). Comparison between

2017 and 2015 is not significant (p = .249; p > 0.05) because difference between average values is 0.02 which is very small.

Cross-variable analyses:

	2014	2015
0 victimisations	2.53(.0197)	2.22(.0216)
1 victimisation	2.9(.0288)	2.6(.0328)
2 victimisations	3.08(.0632)	2.9(.0825)
3 victimisations	3.32(.14)	2.74(.1546)
4 victimisations	-	-

Table 8. Average number of prevention measures used for different number of victimisations, CSEW 2014-2015.

Respondents who were not victimised in year 2014 have used 2.53 prevention measures on average, then this number increased to 2.9 for respondents with a single victimisation, for respondents with two victimisations it was 3.08 prevention measures on average and for respondents with three victimisations it was 3.32. Concluding that, respondents who were more victimised tend to use more prevention measures then respondents who were victimised less times. Same pattern can be seen for year 2015 but with lesser values, because as it was discussed earlier in 2015 the average number of prevention measures used is lower than in 2014.

	2014	2015
0 prevention measures	.135(.0178)	.141(.012)
1 prevention measure	.245(.0159)	.233(.0162)
2 prevention measures	.324(.0166)	.354(.017)
3 prevention measures	.393(.0153)	.387(.0166)
4 prevention measures	.416(.0133)	.383(.013)

Table 9. Average number of victimisations for different number of prevention measures used, CSEW 2014-2015.

In 2014, people who did not use any prevention measures were victimised 0.135 times on average, respondents who used just one prevention measure were victimised 0.245 times, for people with two prevention measures it was 0.324, for three prevention measures 0.393 and for respondents who used four prevention measures the average number of victimisations was 0.416. In 2015, the numbers remain approximately the same, also the same increasing pattern remains. It cannot be concluded that more prevention measures used leads to increased likelihood of victimisation because the survey was conducted post factum, after the incident has happened, however these variables have positive correlations between them. For year 2014 these values were $r > 0$, $r = .141$; sig < 0.05, sig = .000. For 2015 it was *r*

> 0, *r* = .147; sig < 0.05, sig = .000. Nonetheless, positive correlations between these variables does not imply causality between them.

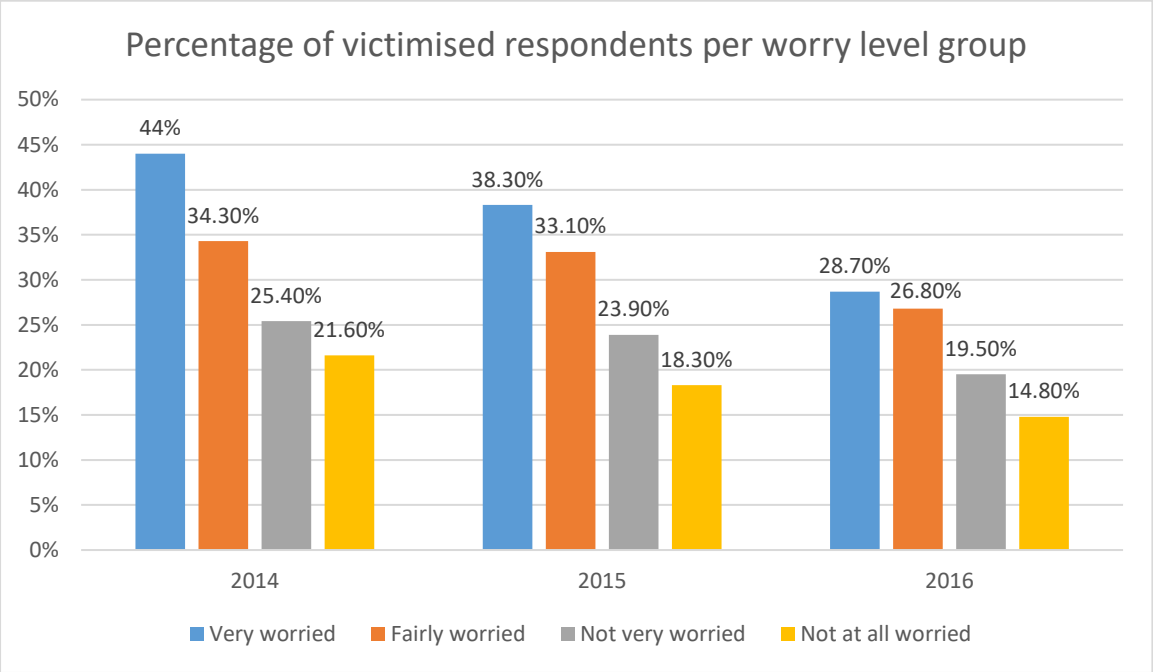


Figure 11. Percentage of victimised respondents per worry level groups, CSEW 2014-2016.

In 2014 the percentage of respondents who were 'Very worried' about being victimised were actually victimised in 44% of cases, 34.3 % 'Fairly worried' respondents were victimised, people who were 'Not very worried' were victimised in 25.4% of cases and percentage of victimised respondents who were 'Not at all worried' was 21.6%. The figure shows that less worried individuals are less likely to be victimised in cyberspace. This same pattern is seen across years 2015 and 2016. Moreover, numbers are dropping, in 2015 percentage of 'Very worried' individuals who were victimised dropped to 38.3% and in 2016 it was 28.7%.

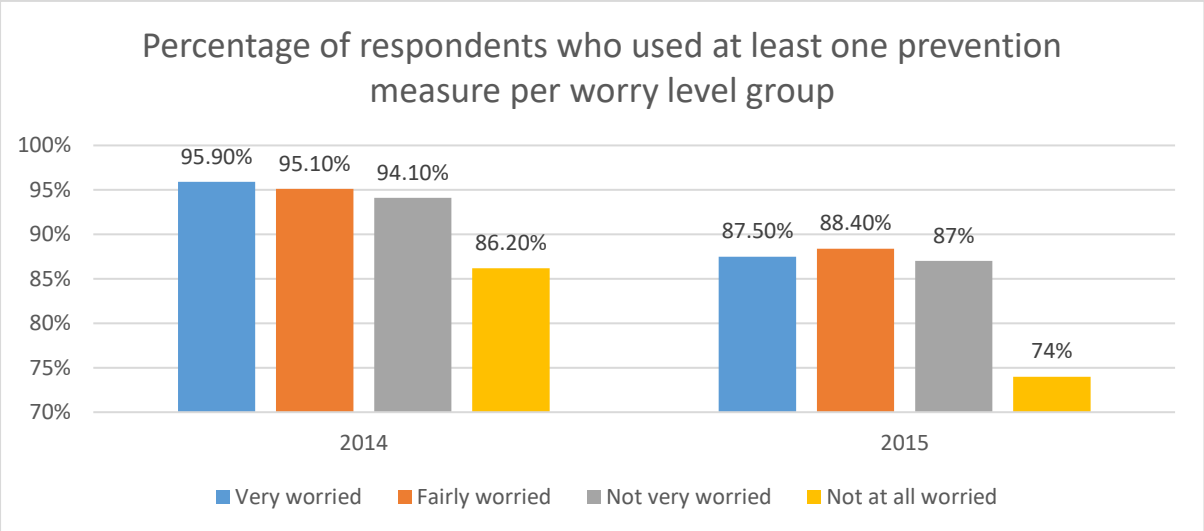


Figure 12. Percentage of respondents who used at least one prevention measure per worry level groups, CSEW 2014-2015.

In 2014 respondents who were concerned about cybercrime (Very worried, Fairly worried and Not very worried) used at least one prevention measure in approximately 95% cases, but individuals who were 'Not at all worried' about being victims of cybercrime used prevention measures in 86.2% of cases. In 2015 the same picture remains, however overall the percentage has also dropped. In 2015 the number of respondents who were 'Not at all worried' and used prevention measures dropped to 74%. Saying that, people who are less worried use less prevention measures, however considering Figure 10 that shows that people who are less worried are less likely to be victimised means that respondents who are less worried use less prevention measures and are less likely to be victimised. This finding can be explained assuming that people who are more concerned about being victims of cybercrime tend to be more reckless in cyberspace and fall into traps such as viruses represented as antiviruses. For example, banner advertisement that says 'clean your computer from viruses for free' leading to a website with a download link of a so-called anti-virus. However, people who are less worried might be less worried because they are more confident and educated about current state of the internet, know what the most effective counter-measures are and are less likely to fall into the traps discussed earlier.

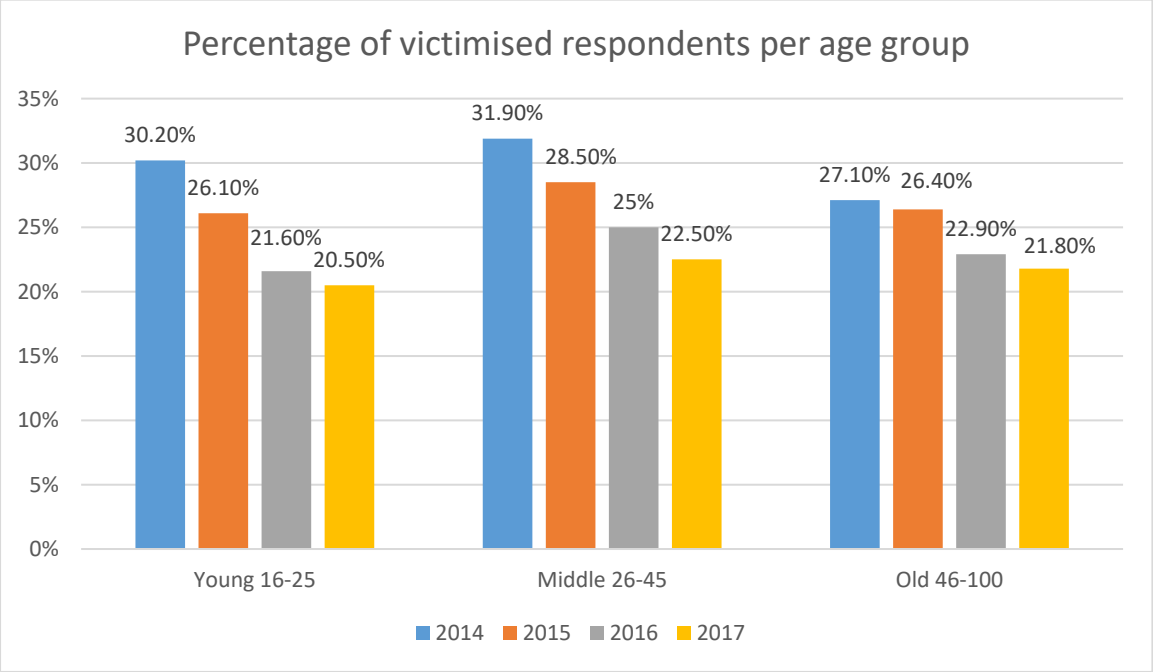


Figure 13. Percentage of victimised respondents per age group, CSEW 2014-2017.

Across all age groups, from young to old people, the proportion of victimised respondents dropped significantly. For young respondents, the percentage has dropped by 9.7%, for middle age group it is 9.4% and 5.3% for old respondents. Comparing between age groups within the same year, it can be noted that middle aged respondents are always approximately 2% more likely to be victimised and the difference between young and old age groups is less notable. However, in 2014, the difference between young and old respondents was 3.1%.

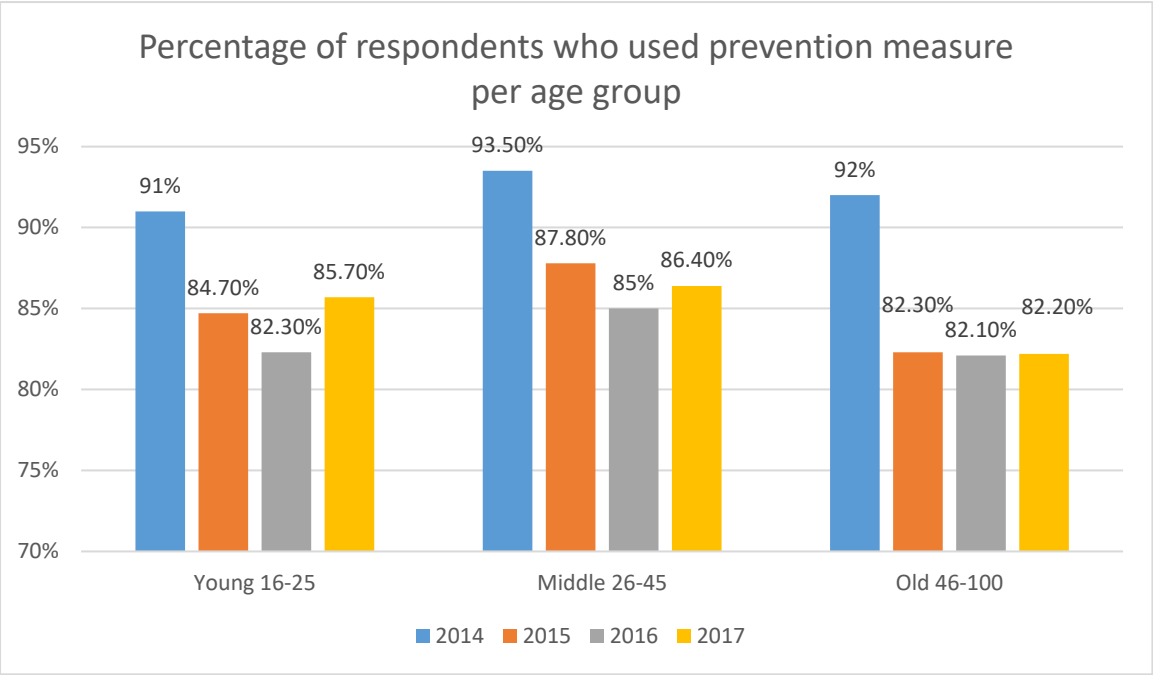


Figure 14. Percentage of respondents who used prevention measure per age group, CSEW 2014-2017.

Figure 14 shows the proportion of individuals within different age groups who have used at least one prevention measure in the four-year period. This same tendency as in Figure 13 of middle aged individuals representing highest proportion of respondents remains, meaning that middle aged respondents are more likely to use prevention measures and are more likely to be victimised. Younger respondents are 2%-3% less likely to use prevention measures than middle-aged groups and groups of older respondents represents the least percentage. However, the pattern across four years for age groups is different. For young and middle-aged groups, the proportion of respondents who use prevention measures dropped by 8.7% and 8.5% from 2014 to 2016 and then grew up again in 2017. However, for the older group of respondents, the percentage dropped from 92% in 2014 to 82.3% in 2015 and then remained almost the same as 82.1% in 2016 and 82.2% in 2017. The older age respondents tend to use prevention measures less often, however rates of victimisation are alike younger age groups who are more likely to use prevention measures.

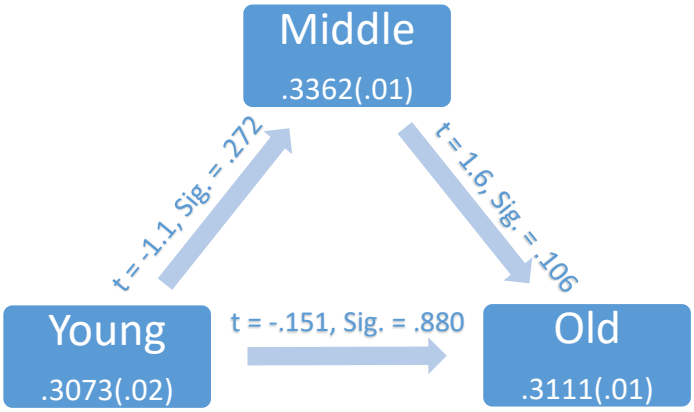


Figure 15. difference significance between age groups and average number of victimisations, CSEW 2015.

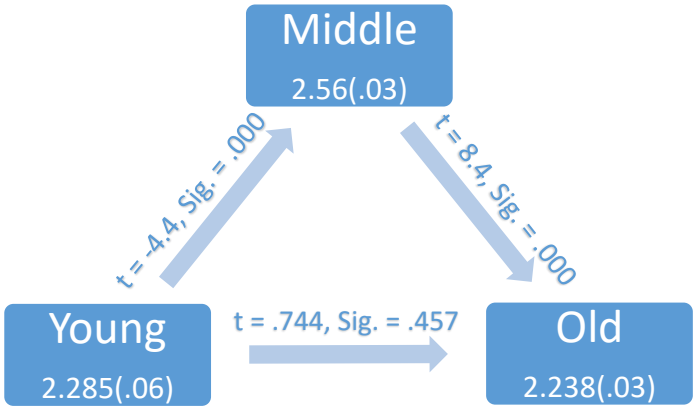


Figure 16. difference significance between age groups and average number of prevention mechanisms used, CSEW 2015.

Figure 15 shows that the young group of respondents had an average victimisation of 0.3073, middle group of people 0.3362 and older respondents 0.3111. ANOVA test confirms that difference between age groups is not significant ($F = 1.477$, $p = 0.228$; $p > 0.05$). Difference between young and middle-aged respondents is not significant ($t = -1.1$, $p = 0.272$; $p > 0.05$), middle and older respondents' difference is not significant ($t = 1.6$, $p = 0.106$; $p > 0.05$) and the difference between young and old respondents is the least significant ($t = -0.151$, $p = 0.880$; $p > 0.05$). Bonferroni post hoc test did not show significant difference between number of victimisations and age groups, confirming t-tests.

Figure 16 carries the same tendency but for use of prevention measures. ANOVA displayed significant difference between age groups ($F = 36.23$, $p = 0.00$; $p < 0.05$). Young aged respondents used 2.285 prevention measures on average, middle aged group of people used 2.56 and older aged respondents used 2.238 prevention measures on average. Figure shows that difference between young and middle aged respondents ($t = -4.4$, $p = 0.000$; $p < 0.05$) and difference between middle and older aged respondents ($t = 8.4$, $p = 0.000$; $p < 0.05$) was significant, however difference between young and old respondents was not ($t = 0.744$, $p = 0.457$; $p > 0.05$). Bonferroni post hoc test confirmed that only difference between young and old age groups is not significant.

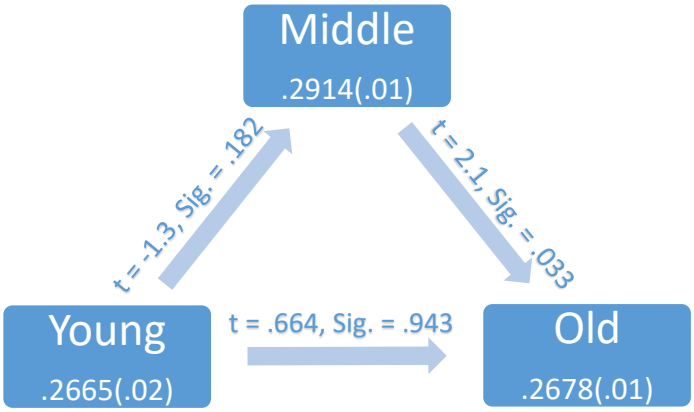


Figure 17. difference significance between age groups and average number of victimisations, CSEW 2016.

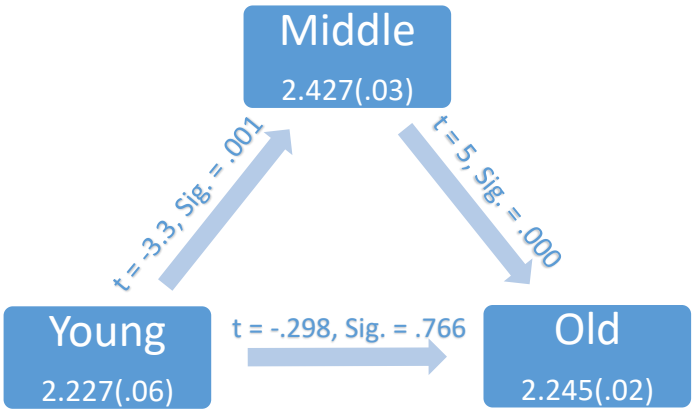


Figure 18. difference significance between age groups and average number of prevention measures used, CSEW 2016.

Figures 17 also shows significant differences between different age groups and the average number of victimisation or average number of prevention measures as Figures 15 but for year 2016. ANOVA test confirms that difference between age groups is not significant (F = 2.465, p = 0.085; p > 0.05). Figure 17 shows that average number of victimisations for young group of respondents in 2016 was 0.2665, 0.2914 for middle-aged group and 0.2678 for older aged people. The difference between the average number of victimisations between young and middle groups of respondents is not significant (*t* = -1.3, p = .182; p > 0.05), the difference between middle and older aged groups is not significant (*t* = 2.1, p = 0.033; p > 0.05) and the difference between young and older aged respondents is the least significant (t = 0.644, p = 0.943; p > 0.05). Bonferroni post hoc test also shows that difference between age groups is not significant.

Figure 18 also shows a significant difference, however between different age groups and the average number of prevention measures used. ANOVA test shows that difference between age groups is significant (F = 13.637, p = 0.000; p < 0.05). The average number of prevention measures used by the young group of people in year 2016 is 2.227, for middle-aged group is 2.427 and for older respondents it is 2.245. The difference between the use of prevention measures between young and middle-aged groups is significant (t = -3.3, p = 0.001; p < 0.05) as well as difference between middle and old aged group of respondents (t = 5, p = 0.000; p < 0.05), however difference between younger and older respondents is not significant (t = -0.298, p = 0.766; p > 0.05). Bonferroni post hoc test also confirms that difference between all age groups but young and old age groups is significant.

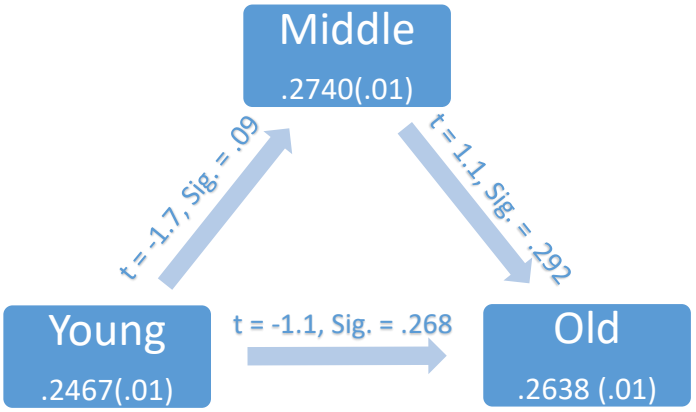


Figure 19. difference significance between age groups and total number of victimisations, CSEW 2017.

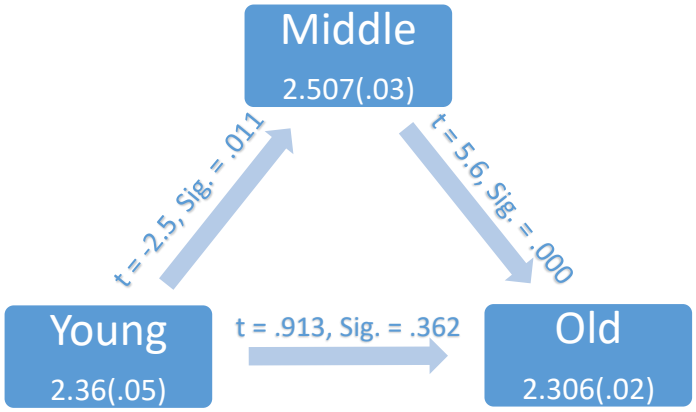


Figure 20. difference significance between age groups and total number of prevention mechanisms used, CSEW 2017.

Figure 19 displays the average number of victimisations for different age groups in year 2017. ANOVA test confirms that difference between age groups is not significant ($F = 1.564$, $p = 0.209$; $p > 0.05$). For younger respondents, the average number of victimisations is 0.2467, for middle-aged group of respondents it is 0.274 and 0.2638 for older respondents. The difference between young and middle-aged groups is very close to being significant, however is not ($t = 1.7$, $p = 0.09$; $p > 0.05$), the difference between middle and older is not significant ($t = 1.1$, $p = 0.292$; $p > 0.05$) and the difference between younger and older respondents also is not significant ($t = -1.1$, $p = 0.268$; sig > 0.05). Bonferroni post hoc test also confirms that there is no significant difference between age groups.

Figure 20 shows a significant difference between age groups and the average number of prevention measures. ANOVA test represents significant difference between age groups ($F = 16.124$; $p = 0.000$; $p < 0.05$). The average number of prevention measures for younger respondents is 2.36, for middle-aged respondents it is 2.507 and 2.306 for older respondents. The difference between these averages is significant in the case of middle and old aged respondents ($t = 5.6$, $p = 0.000$; $p < 0.05$) and between young and middle age groups ($t = -2.5$, $p = 0.011$; $p < 0.05$), however for young and older respondents the difference is not significant ($t = 0.913$, $p = 0.362$; $p > 0.05$). And Bonferroni post hoc test confirms that difference between young and middle, and middle and old age groups is significant, however difference between young and old age groups is not significant.

Summing up, 'Respondents Age' is not significant variable when exploring average victimisation rates, however it is significant when exploring use of prevention mechanisms difference between age groups in case of young and middle, and middle and old aged groups. Nonetheless, difference between younger and older aged respondents is not significant as these groups use almost the same amount of prevention measures on average. Furthermore, it would be most beneficial to conduct a single ANOVA analysis for all years using the year as a separate factor, which might provide further insight and more comprehensive conclusion of a picture as a whole.

		2014	2015	2016		2014	2015	2016
Young	**Several times a day**	95.5%	97.3%	98.1%	**Very worried**	6.2%	4.4%	4.1%
	Two or three times a week	2.5%	1.9%	1.1%	**Fairly worried**	20.9%	20%	24.2%
	Once a week	1.2%	0.5%	0%	**Not very worried**	42.9%	47.2%	47.3%
	Less often than once a week	0.8%	0.3%	0.8%	**Not at all worried**	30%	28.4%	24.4%
Middle	**Several times a day**	90.5%	93.5%	95.1%	**Very worried**	10.3%	10.4%	10.2%
	Two or three times a week	6.4%	4.5%	2.9%	**Fairly worried**	34.4%	34%	35.9%
	Once a week	1.6%	0.6%	0.6%	**Not very worried**	39.4%	39.5%	39%
	Less often than once a week	1.5%	1.3%	1.5%	**Not at all worried**	15.9%	16.1%	15%
Old	**Several times a day**	76.4%	78.6%	80.1%	**Very worried**	8.9%	10.1%	11.4%
	Two or three times a week	14.3%	12.1%	11.5%	**Fairly worried**	33.8%	33.5%	35.6%
	Once a week	3.7%	4.1%	2.9%	**Not very worried**	34.3%	33.9%	34.1%
	Less often than once a week	5.6%	5.2%	5.6%	**Not at all worried**	22.9%	22.5%	19%

Table 10. Relationships between age and use of the internet, and age and worry about being victimised, CSEW 2014-2016.

In 2014, the percentage of respondents was 95.5% and had increased to 98.1% (by 2.6%) in 2016. Moreover, young aged respondents who were not concerned about being victims of cybercrime has dropped from 30% in 2014 to 24.4% in 2016, subsequently the number of concerned respondents has increased. An increase of internet usage can also be noted for middle and old aged respondents, for middle-aged respondents, the number of individuals who have used internet several times a day has increased from 90.5% to 95.1% and for older respondents from 76.4% to 80.1%. However, worry levels for these groups are different. For middle-aged group of respondents percentage almost remained unchanged, only slight difference can be noted; not worried individuals was 15.9% in 2014 then slight increase in

0.2% in 2015 and then decrease to 15% in 2016. For older respondents, the percentage of not at all worried was 22.9% in 2014, then slightly decreased to 22.5% in 2015 and then dropped to 19% in 2016. Older respondents, as well as younger respondents, got more concerned about being victims of cybercrime from 2014 to 2016, however in lesser proportion. That relationship between younger and older respondents' worry level could be explained by an assumption of interaction between these age groups in aspects of internet and technologies in general. Grandchildren might be helping their grandparents understand and set up computers and smartphones for them, sharing their concerns about cybercrime.

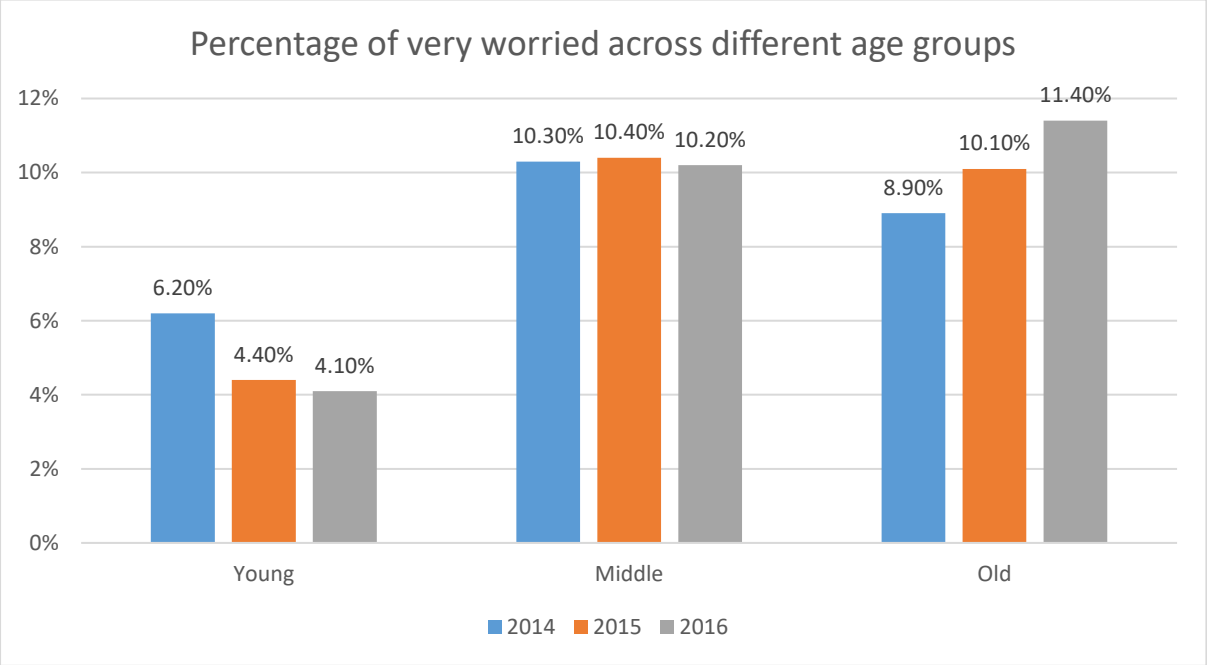


Figure 21. Percentage of very worried across different age groups, CSEW 2014-2016.

The Figure representation makes it clearer to see the percentage of younger people who are very worried about being victims of cybercrime has reduced by 2.1% and percentage of older people who are very worried about being victims of cybercrime has increased by 2.5% over 3 years period, while the percentage of middle-aged respondents remained within 0.2% range.

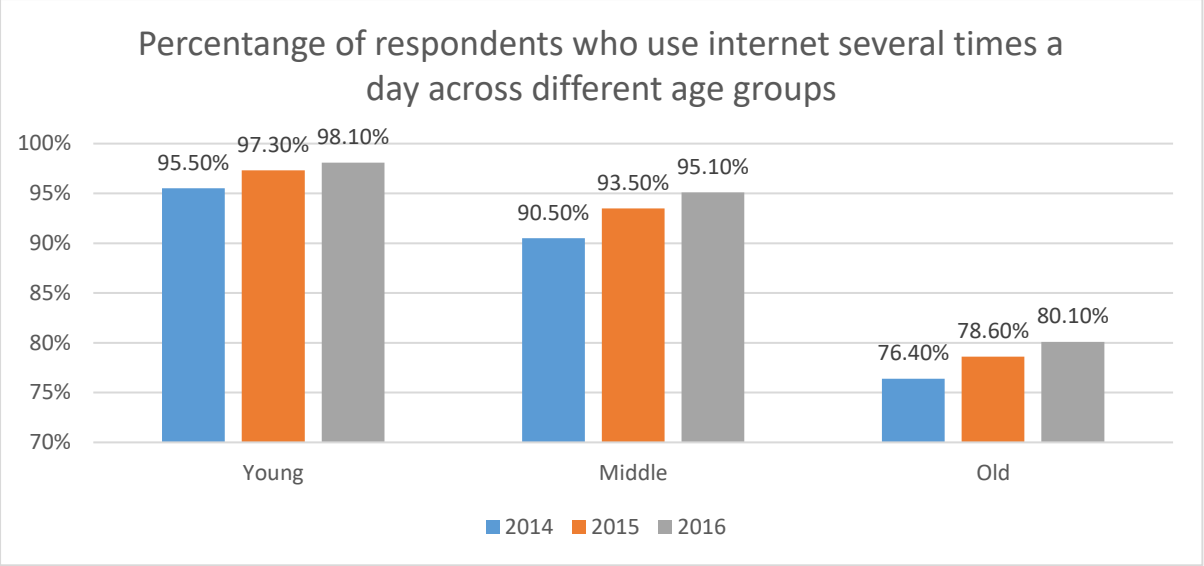


Figure 22. Percentage of respondents who use internet several times a day across different age groups, CSEW 2014-2016.

Figure 22 also demonstrates a visual representation of values set in Table 10, however for the percentage of respondents who use the internet several times a day across different age groups over 3 years period. Diagrams provide vivid image of steady increase in use of the internet several times a day across all age groups. Younger respondents use internet several times a day in 2.6% more cases in year 2016 than in 2014. For middle-aged respondents, that percentage has increased by 4.6% and for older respondent group increase was 3.7%. Livingstone et al. (2011) also stated that with the introduction of different types of entertainment and social activities over the internet, younger people would rather spend more time online than offline.

2014	Worry Level	Percentage of respondents	Victimised	Prevention used mean (Std. Error)
Young	Very worried	6.2%	30.5%	2.7(.18)
	Fairly worried	20.9%	35.8%	2.8(.1)
	Not very worried	42.9%	28.6%	2.7(.07)
	Not at all worried	30%	28.9%	2.5(.09)
Middle	Very worried	10.3%	46.6%	2.6(.08)
	Fairly worried	34.4%	38.7%	2.9(.04)
	Not very worried	39.4%	36.8%	2.9(.04)
	Not at all worried	15.9%	31.4%	2.5(.07)
Old	Very worried	8.9%	43.7%	2.6(.07)
	Fairly worried	33.8%	31%	2.8(.03)

	Not very worried	34.3%	23.5%	2.6(.04)
	Not at all worried	22.9%	18.5%	2(.06)

Table 11. Relationship between worry about being victimised online, actual victimisation and prevention measures used, CSEW 2014.

In 2014, 6.2% of respondents of younger age group were very worried about being victims of cybercrime and 30.5% of them were actually victimised. Furthermore, these 30.5% victimised very worried younger aged respondents used 2.7 prevention measures on average. In the case of the younger aged group, respondents who are 'Fairly worried' are more likely to be victimised, however same 'Fairly worried' individuals use the most prevention measures on average. For middle and old aged respondents, group 'Very worried' is more likely to be victimised, but group 'Fairly worried' still uses the most prevention measures on average. Moreover, for every age group, respondents who are 'Not at all worried' about being victims of cybercrime us the least number of prevention measures on average and are less likely to be victimised. For younger aged group 'Not very worried' respondents are less likely to be victimised with 28.6%, but group 'Not at all worried' is just 0.3% ahead.

2015	Worry Level	Percentage of respondents	Victimised	Prevention used mean (Std. Error)
Young	**Very worried**	4.4%	37%	2.5(.27)
	Fairly worried	20%	32%	2.5(.13)
	Not very worried	47.2%	27%	2.4(.08)
	Not at all worried	28.4%	19.1%	2(.12)
Middle	**Very worried**	10.4%	40.5%	2.5(.09)
	Fairly worried	34%	33.5%	2.7(.05)
	Not very worried	39.5%	24.8%	2.6(.04)
	Not at all worried	16.1%	20.7%	2.2(.07)
Old	**Very worried**	10.1%	37%	2.4(.07)
	Fairly worried	33.5%	33%	2.5(.04)
	Not very worried	33.9%	22.5%	2.4(.04)
	Not at all worried	22.5%	16.5%	1.6(.07)

Table 12. Relationship between worry about being victimised online, actual victimisation and prevention measures used, CSEW 2015.

Table 12 shows the same relationships as Table 11 but for 2015, where the pattern discussed earlier is more evident. For all aged groups, respondents who are the most worried (Very

worried) are most likely to be victimised, on the other hand, respondents who are less worried (Not at all worried) are less likely to be victimised and moreover, use the least prevention measures on average. Another interesting pattern can be noted in both 2014 and 2015 that older aged respondents who are 'Not at all worried' are less likely to be victimised and use the least prevention measures across all age groups. It can be argued that people who are more worried about being victims of cybercrime use more prevention measures than people who are less worried and consequently have higher victimisation rates. It can be explained by the assumption that more worried people are more reckless about installing different prevention measures that they see advertised online that themselves are malwares. At the same time, people who are less worried use slightly less prevention measures on average but most likely are more educated about the state of things on the internet and make more educated choices on the account of which prevention measures to use. However, further and more in-depth research is needed to make a certain conclusion.

2016	Worry Level	Percentage of respondents	Victimised
Young	Very worried	4.1%	7.1%
	Fairly worried	24.2%	31.2%
	Not very worried	47.3%	18.9%
	Not at all worried	24.4%	19.2%
Middle	Very worried	10.2%	40.2%
	Fairly worried	35.9%	28.8%
	Not very worried	39%	21.9%
	Not at all worried	15%	18.7%
Old	Very worried	11.4%	23.6%
	Fairly worried	35.6%	25.2%
	Not very worried	14.1%	17.9%
	Not at all worried	19%	10.5%

Table 13. Relationship between worry about being victimised online and actual victimisation, CSEW 2016.

Table 13 also provides data on relationships between worry about being victimised online and actual victimisation, however the CSEW for 2016 lacks data on the average number of prevention measures used for these groups. Also, the abovementioned pattern is less evident because of the sample size - only 14 respondents of younger aged group were 'Very worried' and just one was victimised making it 7.1%, which makes it unreliable. For middle-aged group, majority of respondents were 'Not very worried' making it 39%, however 'Very worried'

respondents were still most likely to be victimised. In addition, for older-aged group ‘Fairly worried’ respondents were making the most and were most likely to be victimised. However, the pattern where older respondents who are ‘Not at all worried’ are less likely to be victimised remain in 2016.

Regression analyses:

	2014		2015		2016		2017	
Dependent variable: Total number of victimisations	**R^2 = .054**		**R^2 =.009**		**R^2 =.01**		**R^2 =.002**	
Independent variables	**B**	**P**	**B**	**P**	**B**	**P**	**B**	**P**
Constant	.413	.000	.331	.000	.288	.000	.263	.000
Respondents age	-.047	.000	-.008	.473	-.008	.307	.002	.781
Dependent variable: Total number of prevention mechanisms used	**R^2 = .057**		**R^2 =.061**		**R^2 =.028**		**R^2 =.042**	
Independent variables	**B**	**P**	**B**	**P**	**B**	**P**	**B**	**P**
Constant	2.802	.000	2.547	.000	2.397	.000	2.515	.000
Respondents age	-.107	.000	-.130	.000	-.061	.018	-.089	.000

Table 14. How respondents age affects number of victimisations and number of prevention measures used, CSEW 2014-2017.

The regression shows that in 2014, only 5.4% of victimisation cases were affected by the age factor (R^2 = .054), in 2015 the percentage has drastically decreased to 0.9% (R^2 = .009), then in 2016 slightly increased to 1% (R^2 = .01) and in 2017 dropped to 0.2% (R^2 = .002). Moreover, independent variable 'Respondents Age' is only significant in year 2014 ($p < 0.05$; $p = .000$) and only explains 5.4% of cases. Another regression is case where dependent variable is total number of prevention mechanisms used and independent variable is the same – respondents' age. In 2014 age variable affects total number of prevention mechanisms used in 5.7% of cases (R^2 = .057), in 2015 that percentage has increased to 6.1% (R^2 = .061), then in 2016 dropped to 2.8% (R^2 = .028) and increased again in 2017 to 4.2% (R^2 = .042). In this regression variable 'Respondents Age' is significant in all years ($p < 0.05$). To conclude, linear regression analysis with 'Respondents Age' group as independent variable showed that respondents' age variable explains only small percentage of cases. It is a consequence of relationship between these groups not being linear as it can be noted on Figure 13 and Figure 14. Younger and older aged groups tend to have less number of victimisations and use less prevention measures than middle aged groups making it non-linear. If older aged group of respondents had been more victimised and used more prevention measures than middle aged group making it positive linear increase, then linear regression where respondents age is independent variable would have explained more cases.

	2014		2015	
Dependent variable: Total number of victimisations	**R^2 = .212**		**R^2 =.206**	
Independent variables	**B**	**P**	**B**	**P**
Constant	.523	.000	.482	.000
Total number of prevention mechanisms used	.043	.000	.036	.000
What is your personal gross income	.001	.642	.006	.024
Respondents age	-.026	.097	-.010	.543
Are you a student at university or college	-.033	.347	-.061	.076
Type of area: urban/rural	-.034	.135	.006	.778
Respondents sex	-.078	.000	-.056	.004
On average how often do you use the internet	-.087	.000	-.040	.066
How worried are you about being a victim of online crime	-.098	.000	-.109	.000

Table 15. How different factors affect total number of victimisations, CSEW 2014-2015.

Further analysis of linear regression with different independent variables for years 2014 and 2015 was conducted in Table 15. In this case, dependent variable is 'Total number of victimisations' with constant of .523 and R^2 = .212 in 2014 and constant of .482 and R^2 = .206 in 2015 meaning that dependent variable was affected by independent variable in 21.2% of cases in 2014 and 20.6% of cases in 2015. Exploring the table, it can be noted that only several independent variable significantly affected dependent variable (p = .000, in green colour). In 2014 one of these variable was 'Total number of prevention mechanisms used' and had positively affected constant increasing it by B = .043, other significant variables had negative impact on constant decreasing it by the number in 'B' column. In 2015 variable 'On average how often do you use the internet' was not significant anymore, however other variable that were significant in 2014 remained significant. Moreover, variable 'What is your personal gross income' was not significant in 2014 but then became significant in 2015 ($p < 0.05$; p = .024). Reviewing just significant variables, it can be concluded that in 2014 respondents who used one prevention measure had increased total number of victimisations and respondents who were female, used internet two or three times a week or less and were fairly or less worried about being victims of online crime had reduced total number of victimisations. In year 2015 picture is the same, however use of internet is no longer a significant variable and personal gross income is significant.

	2014		2015	
Dependent variable: Total number of prevention mechanisms used	**R^2 = .359**		**R^2 =.350**	
Independent variables	**B**	**P**	**B**	**P**
Constant	2.867	.000	2.379	.000
Total number of victimisations	.156	.000	.166	.000
What is your personal gross income	.063	.000	.074	.000
Type of area: urban/rural	.023	.591	.080	.103
Respondents sex	-.035	.336	.020	.631
Respondents age	-.088	.003	-.066	.048
How worried are you about being a victim of online crime	-.100	.000	-.106	.000
Are you a student at university or college	-.129	.053	-.069	.346
On average how often do you use the internet	-.532	.000	-.630	.000

Table 16. How different factors affect total number of prevention mechanisms used, CSEW 2014-2015.

Table 16 also provides more in-depth linear regression analysis of how the same independent variables as in Table 15 affect the dependent variable, however variables 'Total number of prevention mechanisms used' and 'Total number of victimisations' have been swapped. Number of prevention measures used is now the dependent variable with constant B = 2.867 and R^2 = .359 in 2014 meaning that 35.9% of total number of prevention mechanisms used cases were affected by the list of independent variables; in 2015 that percentage was 35% (R^2 = .350) and constant was B = 2.379. Summing up data demonstrated in the table, it can be concluded that respondents who were victimised once or more and had personal income of £5,000 or more used increased number of prevention mechanisms. But respondents who were female, who were fairly or less worried about being a victim of online crime and used internet two or three times a week or less used decreased number of prevention mechanisms.

		2014		2015	
Model 1	**Dependent variable: Total number of victimisations**	**R^2 = .143**		**R^2 = .164**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	.539	.000	.533	.000
	How worried are you about being a victim of online crime	-.102	.000	-.155	.000
Model 2	**Dependent variable: Total number of victimisations**	**R^2 = .182**		**R^2 = .192**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	.363	.000	.404	.000
	How worried are you about being a victim of online crime	-.094	.000	-.108	.000
	Total number of prevention mechanisms used	.057	.000	.045	.000

Model 3	**Dependent variable: Total number of victimisations**	**R^2 = .198**		**R^2 = .198**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	.411	.000	.438	.000
	How worried are you about being a victim of online crime	-.094	.000	-.109	.000
	Total number of prevention mechanisms used	.045	.000	.044	.000
	On average how often do you use the internet/ Respondents sex	-.093	.000	-.059	.002
Model 4	**Dependent variable: Total number of victimisations**	**R^2 = .208**		**R^2 = .201**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	.455	.000	.454	.000
	How worried are you about being a victim of online crime	-.095	.000	-.109	.000
	Total number of prevention mechanisms used	.044	.000	.040	.000
	On average how often do you use the internet	-.093	.000	-.047	.029
	Respondents sex	-.077	.000	-.059	.002
Model 5	**Dependent variable: Total number of victimisations**	**R^2 = .210**		**R^2 = .204**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	.496	.000	.418	.000
	How worried are you about being a victim of online crime	-.097	.000	-.108	.000
	Total number of prevention mechanisms used	.044	.000	.037	.000
	On average how often do you use the internet	-.088	.000	-.044	.042
	Respondents sex	-.077	.000	-.054	.005
	Respondents age/What is your personal gross income	-.029	.047	.005	.047

Table 17. Stepwise linear regression with 'Total Number of Victimisations' as dependent variable, CSEW 2014-2015.

Stepwise linear regression analysis was conducted to regress multiple variables simultaneously removing non-significant variables, making it clearer which variables are the most important. Analysing Table 17, it can be noted that just one factor 'worry level' explains 14.3% (R^2 = .143) of cases in 2014 and 16.4% (R^2 = .164) of cases in 2015. Looking at year 2014, adding variable 'number of prevention measures used' increased percentage of cases by 3.9% from 14.3% to 18.2% (R^2 = .182), however further models where more factors are added provide significantly lower increase in percentage of cases explained. For year 2015, percentages in proportion are approximately the same. Saying that, it can be proposed that most successful model is 'Model 2' with independent variables 'How worried are you about being a victim of online crime' and 'Total Number of Prevention Measures Used' and these factors are most important to address when discussing change in 'Total Number of Victimisations'.

		2014		2015	
Model 1	**Dependent variable: Total number of prevention mechanisms used**	**R^2 = .279**		**R^2 = .257**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	3.004	.000	2.729	.000
	On average how often do you use the internet	-.637	.000	-.750	.000
Model 2	**Dependent variable: Total number of prevention mechanisms used**	**R^2 = .336**		**R^2 = .331**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	2.544	.000	2.151	.000
	On average how often do you use the internet	-.578	.000	-.688	.000
	What is your personal gross income	.061	.000	.074	.000
Model 3	**Dependent variable: Total number of prevention mechanisms used**	**R^2 = .348**		**R^2 = .342**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	2.478	.000	2.097	.000
	On average how often do you use the internet	-.556	.000	-.653	.000
	What is your personal gross income	.060	.000	.072	.000
	Total number of victimisations	.181	.000	.191	.000
Model 4	**Dependent variable: Total number of prevention mechanisms used**	**R^2 = .354**		**R^2 = .348**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	2.643	.000	2.269	.000
	On average how often do you use the internet	-.555	.000	-.647	.000
	What is your personal gross income	.059	.000	.071	.000
	Total number of victimisations	.162	.000	.168	.000
	How worried are you about being a victim of online crime	-.093	.000	-.100	.000
Model 5	**Dependent variable: Total number of prevention mechanisms used**	**R^2 = .358**		**R^2 = .349**	
	Independent variables	**B**	**P**	**B**	**P**
	Constant	2.749	.000	2.348	.000
	On average how often do you use the internet	-.534	.000	-.629	.000
	What is your personal gross income	.063	.000	.073	.000
	Total number of victimisations	.159	.000	.167	.000
	How worried are you about being a victim of online crime	-.100	.000	-.106	.000
	Respondents age	-.097	.001	-.067	.043

Table 18. Stepwise linear regression with 'Total Number of Prevention Mechanisms Used' as dependent variable, CSEW 2014-2015.

Table 18 also provides stepwise linear regression analysis, however dependent variable now is 'Total Number of Prevention Mechanisms Used'. The picture remains the same as for Table 17, however the variables are different. In 2014 one factor 'On average how often do you use the internet' had explained 27.9% (R^2 = .279) of 'Total Number of Prevention Mechanisms Used' case and 'Model 2' where variable 'What is your personal gross income' was added had increased by 5.7% explained 33.6% (R^2 = .336) cases. Further models, as in Table 17 provided less than one percent increase making it not significant in comparison to difference between 'Model 1' and 'Model 2'. For year 2015 pattern remained the same. Summing up, 'Model 2' where independent variables are 'On average how often do you use the Internet' and 'What is your personal gross income' are most relevant when exploring change in variable 'Total Number of Prevention Mechanisms Used'.

To summarise regression analyses section, it is important to underline that main purpose of this section is to explore different combination of factors and how they affect victimisation rates and use of prevention measures. As it was discussed in the 'Literature Review' section, change in use of prevention measures and actual victimisation in cyberspace can be affected by many different reasons. Regressions allow the possibility to study groups of different factors, establishing the most significant ones. Also, a regression makes it possible to identify factors that are only significant when explored outside of the model and, moreover, lose their significance when grouped with other factors. Identifying such factors is useful for an exploratory study because it provides new ideas and inspirations for further research in the field. Saying that, linear regression analyses have their limitations. For example, it is only limited to linear relationships, assuming that there is straight line between variables. Both dependent and independent variables in this particular study are complicated variables allowing a possibility for non-linear relationships between them. Moreover, linear regression analyses are sensitive for extreme cases and for more precise regression results it would be most beneficial to address influential points of the data.

RESULTS

To summarise the analyses section, different factors and variables were discussed in comparison to victimisation rates online and cybercrime prevention measures used. Firstly, descriptive analyses were carried out to figure out actual data and how it changed over time. Key variables for descriptive analyses are: how worried are people about cybercrime, how often do they use the internet, what are online victimisation rates, what types of cybercrime do respondents experience the most, and the number of prevention measures used. After values mentioned above were established, further in-depth analyses were carried out to calculate if the change in the variables over the years was statistically significant. Subsequently, these variables were compared with each other to establish relationships. For example, how the number of victimisations affected the number of prevention measures used and vice versa, how worry level affected victimisation rates or how victimisation rates and use of prevention measures differs between age groups. The final section of the analyses is in the form of regressions to explore variables that were actually significant in relation to

'total number of victimisations' in the first case and in relation to 'total number of prevention mechanisms used' in the second case.

The first section of the analyses starts with an exploration of how worried respondents were about being victimised online, as it provides description of the 'fear of crime' situation in cyberspace. According to Table 1 and Figure 1 it can be concluded that worry level was increasing from 2014 to 2016 and then slightly lowered in 2017. The number of worried respondents in the UK was approximately 40% each year, however Baker (2013) stated that 76% of internet users in the EU are concerned of cybercrime victimization and moreover, GFI Software Corporation's (2015) independent study showed that 71.5% of U.S. citizens were worried about cybercrime. As such, it can be argued that people in the UK are less worried about cybercrime than people in the EU or the U.S. Followed by Figure 2 and Table 2 where it was established that use of the internet is steadily increasing over the years with a 2% increase in each year. Bomhold (2013) surveyed undergraduate students in the U.S. on the subject of using smartphones to access academic information online and had concluded that 76% of students use internet on their smartphones. Moreover, looking at 'use of the internet' data provided in Figure 2, it can be noted that 76.9% of respondents have used the internet. Figure 3 and 4 look deeper at the 'use of the internet', exploring how often respondents use the internet over the years and it can be concluded that not only do people use the internet more in general, but they also use it more often. The number of respondents who use the internet several times a day is steadily increasing and the number of respondents who use it less often steadily goes down.

Following the structure established in the 'Literature Review' section, exposure to cybercrime in the form of cyberspace victimisation will now be discussed. Looking at Table 3 and Figure 5 it can be seen that the percentage of respondents who were victimised has dropped by 13% over a 7-year period. Furthermore, Table 4 represents data on the average number of victimisations per respondents, which also has dropped by 0.13 incidents. Goucher (2010), who analysed different countries, found that 65% of respondents were victimised, however in Table 3 it can be noted that only 34.9% of respondents were victimised in the UK in 2011. Figure 6 explores changes in particular types of cybercrime and shows a decrease in technological cybercrime such as 'computer virus' and an increase in human interaction cybercrime such as 'online harassment'. Figure 7 explores the significance of the change of victimisation rates over the 7-year period and it can be concluded that the change in victimisation rates gets more significant over the years. The last part of the descriptive section explores use of prevention measures by respondents. Table 5 and Figure 8 show how use of prevention measures changed from 2014 to 2017. The number of respondents who did not use any prevention measures has increased by 8.4% and the number of respondents who used 4 prevention measures has dropped by 5.4%. Figure 9 provides a more in-depth look into use of particular prevention measures from 2014 to 2017 followed by the Table 6 explaining why use of prevention numbers might be falling. Figure 10 provides confirmation that the change in use of prevention measures over the years is mostly significant.

The second part of the analyses provides cross-variable analyses looking into relationships between different variables, with a purpose to explore the 'prevention' side of the argument

discussed in the 'Literature Review' section. Table 9 presents a positive correlation between the variables 'average number of victimisations' and 'number of prevention measures used' demonstrating a higher average number of victimisations for respondents who use a higher amount of prevention measures. Figures 11 and 12 explore how respondents' worry level affects victimisation rates and use of prevention measures. It can be noted that respondents who are less concerned about cybercrime are less likely to use prevention measures and, moreover, are less likely to be victimised. Further in the research, Figures 13 and 14 provide data on how variable 'age' affects victimisation rates and use of prevention measures. It was found that middle-aged respondents are more likely to use prevention measures and are more likely to be victimised while young and old-aged respondents share approximately the same percentages. Exploring significant differences between age groups in relation to variables 'average number of victimisations' and 'number of prevention measures used', it was concluded that the difference between all age groups in relation to victimisation rates is not significant, however the difference between young and old age groups is the least significant. Furthermore, the difference between age groups in relation to use of prevention measures shows that difference between young and middle, and middle and old age groups, is significant, while difference between young and old age groups is not significant. This explains why the difference in victimisation rates between young and old age groups is the least significant. Following this, Table 10 and Figures 21 and 22 present change in worry levels and use of prevention measures over the years across different age groups more clearly and lead to a conclusion that young respondents are getting less worried, older respondents are getting more worried, while the middle-aged groups' worry level remains the same. Moreover, use of the internet is steadily increasing across all age groups. Followed by Tables 11, 12 and 13 that group all variables 'age', 'worry level' and 'use of prevention measures' together making it clear to see that respondents who are more worried about being victims of cybercrime use more prevention measures and consequently getting more victimised.

The last section of analyses consists of linear regressions and stepwise linear regressions with a purpose of establishing the significance of different factors affecting cybercrime victimisation or prevention over the years. However, this final section of the 'Analyses' chapter is more aimed at proposing and exploring different factors that might be significant for a further cybercrime aimed researches, rather than establishing clear causalities, connections and relationships. In Table 14, the variable 'respondents age' is compared to dependent variables 'total number of victimisations' and 'total number of prevention measures used' from 2014 to 2017 and leads to a conclusion that the age of respondents explains only a small percentage of cases and sometimes the percentage is so small that it is no longer significant. Further, Tables 15 and 16's other independent variables are put against the same dependent variable as in Table 14; more significant variables that impact 'number of victimisations' and 'use of prevention measures' were established. Finally, Tables 17 and 18, where stepwise regression analysis was conducted, provide a more in-depth look into which independent variables would be most meaningful in explaining the dependent variables. In the case of cybercrime victimisation, the most important factors to explore would be 'level of worry about cybercrime' and 'number of prevention measures used'. In the case

of the use of prevention measures in cyberspace, the most important factors to explore would be 'how often the internet is being used' and 'level of income'.

DISCUSSION

Conducting descriptive analyses, it was established that use of the internet is steadily increasing from 2011 to 2017. Subsequently, worry of being victimised online is also growing (with exception of the year 2017, where it has decreased). The percentage of victimised respondents is lowering as well as the percentage of respondents who use at least one prevention measure. A decline in the percentage of victimised people and a decline in the use of prevention measures could also reflect a reduction or increase in the fear of cybercrime. As it was established, worry of cybercrime is growing, however rates of victimisation and use of prevention measures are decreasing. It could be argued that increased worry of being victimised in cyberspace makes people more cautious in cyberspace and subsequently use less but more effective prevention measures which renders them less likely to be victimised. However, further research where fear of cybercrime and awareness of cybersecurity measures are distinguished must be conducted in order to establish connections and relationships between fear, victimisation and the prevention of crime in cyberspace.

Putting variables worry, victimisation and prevention of cybercrime against each other, it was proposed that respondents who are victimised more use more prevention measures. Moreover, people who are more concerned about being victims of cybercrime use more prevention measures and are more likely to be victimised, when people who are less worried use less prevention measures and are less likely to be victimised. When comparing the demographic variable 'age of respondent' to use of prevention measures and victimisation rates, it was found out that the middle-aged group used more prevention measures, subsequently getting more victimised, while the young and old-aged used less prevention measures and were less victimised. However, further in the research it was established that age only explains less than 6.1% of cases for both 'use' and 'victimisation'. Finally, conducting stepwise regression analyses, the conclusion was made that in the case of the dependent variable being 'total number of victimisations', the most important independent variables to explore are 'how worried are you about being a victim of online crime' and 'total number of prevention mechanisms used'. In the case of the dependent variable being 'total number of prevention mechanisms used', the essential factors to explore are 'on average how often do you use the internet' and 'what is your personal gross income'.

Secondly, the Crime Survey for England and Wales (CSEW) was chosen as a data set to be analysed mainly because it provides an enormous sample size and the survey itself is conducted by professionals funded by the government. However, the CSEW is not a survey that is specifically aimed to analyse issues of cyberspace, thus the cybercrime section of the survey is not very thorough and CSEW researchers started to develop the cybercrime section only a few years ago, which makes it complicated to compare earlier years to current years because the survey questions differ considerably. Considering the limitations of the used (CSEW) survey, this particular study carries out exploratory character with a purpose to

provide an overview of the current cyberspace situation in England and Wales. It should also be noted that drawing conclusions out of such a limited dataset leads to conclusions being limited and only of an exploratory nature. To improve the reliability and comprehensiveness of the study, it would be highly beneficial to explore a survey that is designed to explore cyberspace specifically and, moreover, explore surveys conducted in different countries as cybercrime is locked at the specific region and more often is an international matter. For example, studies conducted by the European Commission called Special Eurobarometer include surveys aimed specifically at the cyber security and cybercrime issue. Moreover, Special Eurobarometer is one of the very few comprehensive cybercrime surveys. Firstly, it is aimed to explore cyberspace, secondly, provide sizeable sample size of almost 30,000 respondents, thirdly and most importantly, it covers most of the European Union countries, making this survey international which is highly beneficial for a cybercrime research.

Another option would be to design one's own survey where questions are specifically built around a particular cybercrime issue that is being studied, however it would eliminate the option to study and compare different years. Designing one's own survey would also be beneficial for the sample size as it would be possible to distribute the questionnaire online, targeting individuals who already are in the internet environment and are more likely to be educated about cybercrime matters and thus provide more insight.

In addition, the main research question is based around factors that shape victimisation online and, moreover, impact peoples' use of prevention measures in cyberspace. However, it only states which factors are more significant than others in explaining the number of victimisations and number of prevention measures used, but the study does not cover why exactly certain factors such as 'age of internet user' are only significant in such a small amount of cases. It would also be advantageous to explore the exact reasons behind people who use the internet more often using more prevention measures on average. Furthermore, the analysed data set does not consider in-build prevention measures that become more prevalent in contemporary technologies. It might be a case where people who use most prevention measures are more likely to be victimised because in the survey only prevention measures they have consciously downloaded and installed are mentioned, however it might be the only prevention measures that are supported by official software and hardware developers.

For further research in the field, it would be most useful to split this research topic into sub-topics and analyse these issues separately and in more detail. Firstly, studying how exactly fear of cybercrime is constructed and how the impact of cybercrime being misrepresented in the media will assist in understanding of what can be done to reduce worry of cybercrime. Secondly, analysing use of prevention measures in cyberspace in detail would be highly beneficial as it will provide insight into which exact prevention measures people use and the reasons behind it. Analysing acknowledgement of in-built prevention measures would also prove useful as it would provide more certainty on why people who use more prevention measures are more likely to be victimised in cyberspace. However, it would require a more comprehensive and narrow subject-focused research study to be able to make suggestions in regards to cybercrime prevention improvements. Though it was mentioned earlier, this

particular study is of an exploratory character aimed at identifying these narrow subjects, which might be important to study more thoroughly if the aim is to make actual proposals with regards to cybercrime prevention.

CONCLUSION

To summarise the research, in spite of exciting research results regarding the discovery of the most impactful factors in relation to number of victimisation and number of prevention measures used in cyberspace, there is still enough of room for criticism and improvement in relation to the data set used, how analyses were conducted and how findings were interpreted. Further, in this section, findings of the research are going to be summarised, suggestions for a further research in the topic are going to be made as well as speculations about possible practical implications of the research findings.

Firstly, in the course of this study it was established that the general population of the UK is getting more familiar and more comfortable with the internet and the use of the internet amongst people in the UK is rapidly increasing. Nonetheless, fear of cybercrime is also growing as people trust the internet with more of their personal information such as banking details in the case of mobile banking applications being introduced, or personal information such as friends, interests and current location in case of social media applications advancements. However, victimisation rates are lowering significantly over the years and use of prevention measures is increasing. Such explorative data was only possible to be obtained by employing a quantitative approach as it allows studying trends for general population.

Secondly, it was stated that factors such as 'worry of cybercrime' and 'number of prevention measures used' affect the number of victimisations online most significantly. People who are more worried about cybercrime and use more prevention measures online are more likely to be victimised in cyberspace. While this statement might be counter-intuitive, it can be explained by reviewing people's choice of prevention measures. Assumption is that person who uses just one but assured and certified prevention measure is less likely to be victimised than a person who would use dozen of unverified prevention tools, which might be concealed malwares themselves. To confirm such hypothesis further analysis is required. Saying that, these are the two main factors that should be addressed when aiming to reduce victimisation in cyberspace. As it was discussed earlier, studies that are represented in different media sources claim cybercrime victimisation to be as high as 80%, which highly differs from self-reported victimisation data provided by the CSEW survey as it was found in the analyses section of this study. Misrepresentation of the state of actual cybercrime can lead to increased fear of cybercrime that can subsequently cause excessive use of unnecessary prevention measures. Different educational and informational guides, presentations and tutorials can have a positive effect on these issues. Revealing actual data on victimisation in cyberspace and demonstrating that cyberspace is much safer than it is perceived to be might reduce fear of cybercrime across the general population. Introducing basic cybersecurity courses in schools, universities and within organisations to educate people of all age groups on the most effective prevention measures online, the most common cyberattacks on a

personal and organisational level, if applicable, and the prevention measures that are actually worth using and which prevention measures are most likely to be malwares themselves. Introducing such programs/courses might significantly reduce cybercrime victimisation rates for the general population and reduce financial damage on a governmental/organisational level.

To conclude the research, it is crucial to pinpoint that this is an exploratory study that aims to explore trends of peoples' behaviour in cyberspace. More specifically, to explore factors that have the most significant impact on peoples' behaviour in relation to victimisation online and use of prevention measures online. Furthermore, it is important to acknowledge that cyberspace is an extraordinarily fast changing environment and studies conducted within the field of cyberspace might become outdated in just a few years as technological progress advances and methods of cyberattack and cybercrime protection techniques change with it.

References

Abel, R. (2017, November 8). *Americans worry about cybercrime more than they worry about car theft.* Retrieved from SC Media The Cybersecurity Source: https://www.scmagazine.com/home/news/cybercrime/americans-worry-about-cybercrime-more-than-they-worry-about-car-theft/

Akhgar, B., & Brewster, B. (2016). *Combatting Cybercrime and Cyberterrorism : Challenges, Trends and Priorities.* Springer.

Almadhoob, A., & Valverde, R. (2014). Cybercrime Prevention in the Kingdom of Bahrain via IT Security Audit Plans. *Journal of Theoretical and Applied Information Technology*, 274-292.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., . . . Savage, S. (2013). Measuring the Cost of Cybercrime. *The Economics of Information Security and Privacy*, 265-300.

Anonymous. (2017). Fighting Cybercrime. *Arkansas Business*, 30.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). *2020 Cybercrime Economic Costs: No Measure No Solution.* Toulouse: 2015 10th International Conference on Availability, Reliability and Security.

B., K. (2016). Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. *Combatting Cybercrime and Cyberterrorism*, 3-15.

Babbie, E. R. (2010). *The Practice of Social Research (12th ed.).* Balmont: Wadsworth Cengage.

Baines, V. (2013). Fighting the Industrialization of Cybercrime. *UN chronicle*, 10-12.

Baker, J. (2013, November 22). *Survey: Most Europeans fear cybercrime but fewer take security measures*. Retrieved from PCWorld: https://www.pcworld.com/article/2066460/survey-most-europeans-fear-cybercrime-but-fewer-take-security-measures.html

Bernik, I. (2014). *Focus Series: Cybercrime and Cyber Warfare.* John Willey & Sons.

Bidgoli, M., & Grossklags, J. (2016). End user cybercrime reporting: what we know and what we can do to improve it. *Cybercrime and Computer Forensic (ICCCF)*, 1-6.

Bomhold, C. (2013). Educational use of smart phone technology: a survey of mobile phone application use by undergraduate university students. *Program: Electronic Library and Information Sytstems*, 424-436.

Bossler, A. M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 400-420.

Buono, L. (2014). Fighting cybercrime through prevention, outreach and awareness raising. *ERA Forum*, 1-8.

Celine, J. (2013). The Philippines Cybercrime Prevention Act. *International Financial Law Review*.

Chen, R.-S., & Ji, C.-H. (2015). Investigating the relationship between thinking style and personal electronic device use and its implications for academic performance. *Computers in Human Behavior*, 177-183.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 308-333.

Choi, K.-S. (2011). Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimisation. In K. Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour* (pp. 229-252). Boca Raton: Taylor & Francis Group.

Choraś, M., Kozik, R., & Maciejewska, I. (2016). Emerging Cyber Security: Bio-inspired Techniques and MITM Detection in IoT. *Combatting Cybercrime and Cyberterrorism*, 193-207.

Choraś, M., Kozik, R., Churchill, A., & Yautsiukhin, A. (2016). Are we doing all the right things to counter cybercrime? *Combatting Cybercrime and Cyberterrorism*, 279-294.

Clarke, R. V., & Cornish, D. B. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending.* Springer.

Computer Misuse Act. (1990). Retrieved from http://www.legislation.gov.uk/ukpga/1990/18

Copeland, J. (2004). Enigma. In A. M. Turing, *The Essential Turing* (pp. 217-352). Oxford: Clarendon Press.

de Graaf, D., Shosha, A. F., & Gladyshev, P. (2012). BREDOLAB: shopping in the cybercrime underworld. *4th International Conference on Digital Forensics & Cyber Crime.* Retrieved from https://ulir.ul.ie/handle/10344/2896

Deloitte. (2015). *Cybersecurity Survey 2015.* Retrieved from Deloitte: https://www2.deloitte.com/ca/en/pages/risk/articles/cybersecurity-survey-2015.html

DeVoe, J., & Murphy, C. (2011). *Student Reports of Bullying and Cyber-Bullying: Results from the 2009 School Crime Supplement to the National Crime Victimization Survey.* National Center for Education Statistics.

Dimc, M., & Dobovsek, B. (2013). Perception of Cybercrime by Selected Internet Users in Slovenia and USA. *Journal of Criminal Justice & Security*, 338-356.

Ditton, J., Bannister, J., Gilchrist, E., & Farrall, S. (1999). Afraid or Angry? Recalibrating the 'Fear' of Crime. *International Review of Victimology*, 83-99.

Dobrinoiu, M. (2014). ID Theft in Cyberspace. *Lex et Scientia*, 117-120.

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, 97-116.

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security*, 5-8.

Evans, M., & Scott, P. (2017, January 19). *Fraud and cyber crime are now the country's most common offences.* Retrieved from Telegraph: https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/

Federal Trade Commission. (2013, April 19). *FTC Survey for 2011 Shows an Estimated 25.6 Million Americans Fell Victim to Fraud*. Retrieved from Federal Trade Commission Government Web site: https://www.ftc.gov/news-events/press-releases/2013/04/ftc-survey-2011-shows-estimated-256-million-americans-fell-victim

Feily, M., & Shahrestani, A. (2009). A Survey of Botnet and Botnet Detection. *2009 Third International Conference on Emerging Security Information, Systems and Technologies* (pp. 268-273). Penang: Universiti Sains Malaysia.

Fick, J. (2009). Prevention is Better than Prosecution: Deepening the Defence against Cyber Crime. *Journal of Digital Forensics, Security and law*.

Financial Fraud Action UK. (2013, March 12). *Decline in fraud losses stalled by rise in deception crime aimed at consumers.* Retrieved from Financial Fraud Action UK.

Frost, & Sulivan. (2014). Smartphone fingerprint biometrics to drive consumer uptake. *Biometric Technology Today*, 1-2.

Fuentes, C., & Svingstedt, A. (2017). Mobile phones and the practice of shopping: A study of how young adults use smartphones to shop. *Journal of Retailing and Consumer Services*, 137-146.

GFI Software. (2015, February 26). *US Cyber Security Survey: Fear of Cyber Crime Up 66 Percent.* Retrieved from CISION: PR Newswire: https://www.prnewswire.com/news-releases/us-cyber-security-survey-fear-of-cyber-crime-up-66-percent-300042043.html

Gibson, M. (2014, January 23). *Cell Phone Statistics: Updated 2013.* Retrieved from Arkadin Collaboration Services: https://www.accuconference.com/blog/cell-phone-statistics-updated-2013/

Goldenbeld, C., Houtenbos, M., Ehlers, E., & De Waard, D. (2012). The use and risk of portable electronic devices while cycling among different age groups. *Journal of Safety Research*, 1-8.

Gooch, G., & Williams, M. (2015). *A Dictionary of Law Enforcement.* Oxford University Press.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security*, 16-18.

Graham, D. (2016). The era of lethal police robots has arrived. *Defense One*.

Gray, D., Citron, D. K., & Rinehart, L. C. (2013). Fighting Cybercrime After "United States v. Jones". *The Journal of Criminal Law and Criminology*, 745-801.

Griffin, R. C. (2012). Cybercrime. *J. Int'l Com. L. & Tech.*, 136.

Halfacree, G. (2014, July 13). *The history of the personal computer - sixty years of desktop progress.* Retrieved from Think Progress: http://www.think-progress.com/blog/innovation-and-entrepreneurship/history-of-the-personal-computer/

Hardawar, D. (2012, March 29). *The magic moment: Smartphones now half of all U.S. mobiles.* Retrieved from Venturebeat: https://venturebeat.com/2012/03/29/the-magic-moment-smartphones-now-half-of-all-u-s-mobiles/

Harris, M., & Singla, R. (2014). Cybercrime Costs. *Accountancy Ireland*, 34-36.

Hernandez-Castro, J., & Boiten, E. (2014). Cybercrime prevalence and impact in the UK. *Computer Fraud & Security*, 5-8.

Hossain, E., & Ahmed, Z. (2016). Academic use of smartphones by university students: a developing country perspective. *The Electronic Library*, 651-665.

House of Lords. (2007). *Personal Internet security, Volume I: report. Science and Technology Committee.* London: The Stationery Office Limited.

Jardine, E. (2015, July 24). Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. *Global Commission on Internet Governance Paper Series*.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 470-486.

Koivunen, M., Niemi, A., & Hupli, M. (2015). The use of electronic devices for communication with colleagues and other healthcare professionals – nursing professionals' perspectives. *Journal of Advanced Nursing*, 620-631.

Koo, C., Chung, N., & Kim, H.-W. (2015). Examining explorative and exploitative uses of smartphones: a user competence perspective. *Information Technology & People*, 133-162.

Kourouthanassis, P. E., & Giaglis, G. M. (2012). Introduction to the special issue mobile commerce: the past, present, and future of mobile commerce research. *International Journal of Electronic Commerce*, 5-18.

Kratchman, S., Jacob, L. S., & Smith, L. M. (2008). The Perpetration and Prevention of Cybercrimes. *Internal Auditing*, 3-8,10,12.

Ladd, D. A., Datta, A., Sarker, S., & Yu, Y. (2010). Trend in mobile computing withing the IS discipline. *Communication of the Association for Information Systems*, 285-306.

Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime prevention*, 157-175.

Leukfeldt, E. R. (2014). Cybercrime and Social Ties. *Trends in Organized Crime*, 231-249.

Li, X. (2007, September). International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Webology*.

Livingstone, S., Haddon, L., Gorzig, A., & Ólafsson, K. (2011). *Risk and Safety on the Internet. The perspective of European Children.* London: EU Kids Online.

Maher, D. (2017). Can artificial intelligence help in the war on cybercrime? *Computer Fraud & Security*, 7-9.

Mahoney, R. (2016). Preventing Cybercrime. *Business NH Magazine*, 20-22.

Mayer, J. (2016). Cybercrime litigation. *University of Pennsylvania law review*, 1480.

McAfee & CSIS. (2014a, June 6). *Stopping Cybercrime can positively.* Retrieved from http://www.mcafee.com/uk/about/news/2014/q2/2014060

McAfee and CSIS. (2014b). *Economic Impact Cybercrime 2.*

McQuade, S. C. (2006). *Understanding and managing cyber crime.* Boston: Pearson/Allyn and Bacon.

Me, G., & Spagnoletti, P. (2005). Situational Crime Prevention and Cyber-crime investigation: the Online Pedo-pornography case study. *EUROCON 2005 - The International Conference on "Computer as a Tool"* (pp. 1064-1067). Belgrade: IEEE.

Mesko, G., & Bernik, I. (2011). Cybercrime: Awareness and Fear. *2011 European Intelligence and Security Informatics Conference* (pp. 28-33). Ljubljana: University of Maribor.

Mills, J. E., & Byun, S. (2006). Cybercrimes against Consumers: Could Biometric Technology Be the Solution? *IEEE Internet Computing*, 64-71.

Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security.* New York: John Wiley and Sons.

Mobasheri, M., Johnston, M., Syed, U. M., King, D., & Darzi, A. (2015). The uses of smartphones and tablet devices in surgery: A systematic review of the literature. *Surgery*, 1352-1371.

Murashbekov, O. B. (2015). Methods for Cybercrime Fighting Improvement in Developed Countries. *The Journal of Internet Banking and Commerce*.

Nasi, M., Oksanen, A., Keipi, T., & Rasanen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 203-210.

National Crime Agency. (2015). Network Security. *Network Security*, 3.

National Highway Traffic Safety Administration. (2016). Effect of Electronic Device Use on Pedestrian Safety: A Literature Review. *Annals of Emergency Medicine*, 233-234.

Nederlandese Vereniging van Banken. (2012). *Dutch Banking Association. Annual Report 2012.* Amsterdam: Nederlandse Vereniging van Banken.

Neuman, L. W. (2002). *Social research methods: Qualitative and Quantitative approaches.*

Neumann, J. V. (1949). *Theory and organization of complicated automata.*

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 773-793.

Norton Antivirus Software. (2012). Cybercrime costs 110bn a year – maybe more. *Computer Fraud & Security*, 3, 20.

Office for National Statistics. (2013, August 8). *Internet access - households and individuals, Great Britain: 2013*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2013-08-08

Office for National Statistics. (2013, September). *Internet Access 2012: Households and individuals.* Retrieved from www.ons.gov.uk/ons/rel/rdit2/Internet-access--households-and-individuals/2012/stb-Internet-access-households-and-individuals–2012.html

Olson, R. L., Hanowski, R. J., Hickman, J. S., & Bocanegra, J. (2009). Driver distraction in commercial vehicle operations. *U.S. Department of Transportation DOT, Federal Motor Carrier Safety Administration FMCSA*.

Owen, T., Noble, W., & Speed, F. C. (2017). *New Perspectives on Cybercrime.* Springer.

Papanikolau, A., Vlachos, V., Papathanasiou, A., Chaiklais, K., Dimou, M., & Karadimou, M. (2013). *Cyber crime in Greece: How bad is it?* Belgrade: 2013 21st Telecommunications Forum Telfor (TELFOR).

Philippsohn, S. (2001). Trends in Cybercrime - An Overview of Current Financial Crimes on the Internet. *Computers and Security*, 53-69.

Police Commissioners' Conference Electronic Crime Working Party. (2000). *The Virtual Horizon: Meeting the Law Enforcement Challenges: Developing an Australasian Law Enforcement Strategy for Dealing With Electronic Crime.* Adelaide: AustralasianCentrefor PolicingResearch.

Rashkovski, D., Naumovski, V., & Naumovski, G. (2016). Cybercrime Tendencies and Legislation in the Republic of Macedonia. *European Journal on Criminal Policy and Research*, 127-151.

Reyns, B., Randa, R., & Henson, B. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety*, 38-59.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2012). Fear of Cyber-Identity Theft and Related Fraudulent Activity. *Psychiatry, Psychology and Law*, 315-328.

Roosendaal, A., Kert, M., Lyle, A., & Gasper, U. (2016). Data Protection Law Compliance for Cybercrime and Cyberterrorism Research. *Combatting Cybercrime and Cyberterrorism*, 81-96.

Rouse, M. (2014, March). *Information Age.* Retrieved from TechTarget: https://searchcio.techtarget.com/definition/Information-Age

Rughiniş, C., & Rughiniş, R. (2014). Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. *Computers & Security*, 111-125.

Scott, K. M., Nerminathan, A., Alexander, S., Phelps, M., & Harrison, A. (2017). Using mobile devices for learning in clinical settings: A mixed-methods study of medical student, physician and patient perspectives. *British Journal of Educational Technology*, 176-190.

Serious Crime Act. (2015). Retrieved from http://www.legislation.gov.uk/ukpga/2015/9

Singleton, T. (2013). Fighting the Cybercrime Plague. *Journal of Corporate Accounting & Finance*, 3-7.

Škařupová, K., Ólafsson, K., & Blinka, L. (2015). The effect of smartphone use on trends in European adolescents' excessive Internet use. *Behaviour & Information Technology*, 68-74.

Spada, M. M. (2014). An overview of problematic Internet use. *Addictive Behaviors*, 3-6.

Statista. (2018a). *Number of smartphone users worldwide from 2014 to 2020.* Retrieved from Statista: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Statista. (2018b). *UK: smartphone ownership by age from 2012-2018.* Retrieved from Statista: https://www.statista.com/statistics/271851/smartphone-owners-in-the-united-kingdom-uk-by-age/

SyndiGate Media Inc. (2018, December 30). The importance of cyber security in modern Internet age. Bahrain.

Thomas, D., & Loader, B. (2000). *Cybercrime: Law neforcement, Security and Surveillance in the Information Age.* London: Routledge.

Tuli, F. (2011). The basis of distinction between qualitative and quantitative research in social science: reflection on ontological, epistemological and methodological perspectives. *Ethiopian Journal of Education and Science*.

United Nations Crime and Justice Information Network. (1999). International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-Related Crime. *International Review of Criminal Policy*, 43-44.

United Nations Office on Drugs and Crime. (2013, February). *Comprehensive Study on Cybercrime.* Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Van Der Wagen, W., & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as hybrid Criminal Actor-Networks. *British Journal of Criminology*, 578-595.

Vanderveen, G. (2006). *Interpreting Fear, Crime, Risk & Unsafety.* The Hague: BJU Legal Publishers.

Viano, E. C. (2017). *Cybercrime, Organized Crime, and Societal Responses.* Springer, Cham.

Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*, 323-338.

Wagenaar, P. (2012). *Detecting Botnets Using File System Indicators.* University of Twente.

Wall, D. (2001). Cybercrimes and the Internet. In D. Wall, *Crime and the Internet.* London: Routledge.

Wall, D. (2005/15). The Internet as a Conduit for Criminal Activity. In A. Pattavina, *Information Technology and the Criminal Justice System* (pp. 77-98). Thousand Oaks: Sage.

Wall, D. S. (2008a). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, 45-63.

Wall, D. S. (2008b). Cybercrime and the Culture of Fear. *Information, Communication & Society*, 861-884.

Wang, D., Xiang, Z., & Fesenmaier, D. R. (2014). Smartphone use in Everyday Life and Travel. *Journal of Travel Research*, 52-63.

Williams, K. C., & Page, R. A. (2011). Marketing to the Generations. *Journal of behavioral Studies in Business*, 1-17.

Woodcock, B., Middletion, A., & Nortcliffe, A. (2012). Considering the smart phone learner: an investigation into student interest in the use of personal technology to enhance their learning. *Student Engagement and Experience Journal*, 1-15.

Wynne, T. (2008). An Investigation into the Fear of Crime: Is there a Link between the Fear of Crime and the Likelihood of Victimisation? *Internet Journal of Criminology*, 1-29.

Yar, M. (2006). *Cybercrime and Society.* SAGE Publications.